Introdução à Teoria dos Números

notas de aula – 2026.07.22.23.30

Jerônimo Pellegrini

id: 4a90c56b5fcaf3a582b041ec15920dd82967e8a9

Com 433 páginas, 120 Definições, 226 Teoremas, 71 Lemas, 3 Proposições, 24 Corolários, 122 Exemplos, 350 Exercícios com 82 dicas ou respostas, 280 notas de rodapé[1], 96 referências bibliográficas. e 433 entradas no índice. Tudo em um só volume!

[1] Um exagero de notas de rodapé! Sem custo adicional!

Este trabalho está disponível sob a licença *Creative Commons Attribution Non-Commercial Share-Alike versão 4.0*.

https://creativecommons.org/licenses/by-nc-sa/4.0/deed.pt_BR

Sumário

Sumário **i**

Nomenclatura **vii**

Parte NVLLA **1**

1 Introdução **3**

2 Números **5**
2.1 Naturais 6
2.1.1 Um modelo para $\mathbb{N}$ 7
2.1.2 Independência dos axiomas 8
2.2 Indução 9
2.2.1 Indução “Forte” 15
2.2.2 Aritmética 17
2.2.3 Ordem 20
2.3 Descida Infinita 24
2.4 Inteiros e Racionais 30
2.4.1 Definições e Modelos 33
2.5 Anéis e Corpos 34

3 Bases **41**
3.1 Naturais 42
3.2 Racionais positivos 45
3.3 A função base 13 de Conway 46

Parte I **54**

4 Divisibilidade **57**
4.1 Divisão 57
4.2 Máximo Divisor Comum 60
4.3 Algoritmo de Euclides para cálculo do MDC 65

4.3.1 Coeficientes de Bézout: algoritmo estendido de Euclides . 68
4.4 Mínimo Múltiplo Comum 70
4.5 Números de Fibonacci 73
4.5.1 Complexidade do algoritmo de Euclides 78
4.6 Domínios Euclideanos: Inteiros Gaussianos e Polinômios 79

5 Primos **93**
5.1 Fatoração Única em $\mathbb{Z}$ 94
5.2 Números de Mersenne e de Fermat 97
5.3 Infinitos primos 102
5.4 $4k+1$, $4k+3$ 107
5.5 Fatoração Única em Dominios Euclideanos 111

6 Congruências **119**
6.1 Relações de congruênca e aritmética modular 119
6.2 Aplicação: critérios de divisibilidade 129
6.2.1 Em bases diferentes 131
6.3 Congruências Lineares e Equações Diofantinas 132
6.4 O Teorema Chinês dos Restos 137
6.4.1 Módulos não co-primos 142
6.5 O Teorema Chinês dos Restos, novamente 146
6.6 Congruências lineares em n variáveis 150
6.7 Congruências polinomiais de qualquer grau 151
6.8 Sequência de Fibonacci módulo m 160

7 Sistemas de Resíduos **167**
7.1 Sistemas completos e reduzidos de resíduos 168
7.2 Raízes primitivas 172
7.3 Raízes primitivas com módulo primo 180
7.4 Grupos 181
7.4.1 O grupo de unidades 187
7.5 Raízes da Unidade 188

8 Funções Aritméticas **199**
8.1 Funções multiplicativas 207
8.2 Números Perfeitos 210
8.3 Convolução de Dirichlet 212
8.4 Função de Mangoldt, $\Lambda(x)$ 222
8.5 Maior Inteiro (chão), $\lfloor x \rfloor$ 224
8.6 $\pi(n)$ 229
8.7 Crescimento de $\pi(n)$ 230

9 Resíduos Quadráticos **241**
9.1 Resíduos Quadráticos 241
9.2 Reciprocidade Quadrática 245
9.2.1 Demonstração de Gauss (a primeira, por indução) – rascunho 250
9.2.2 Demonstração de Rousseau 251
9.2.3 Demonstração Geométrica de Eisenstein 254
9.2.4 Demonstração de Gauss (a quarta, usando raízes da unidade) 260
9.3 Método para resolução de congruências quadráticas 265
9.3.1 Módulo primo 265
9.3.2 Módulo potência de primo 266
9.3.3 Módulo composto 267
9.3.4 Equação geral do segundo grau 268

10 Soma de Quadrados **273**
10.1 Soma de dois quadrados 273
10.2 Soma de quatro quadrados 279
10.3 Soma de três quadrados 283
10.4 Quantidade de representações 286

Parte II **293**

11 Formas Quadráticas **295**
11.1 Formas Bilineares e Quadráticas 295
11.1.1 Representação de inteiros e equivalência de formas . . . 300
11.2 Formas quadráticas binárias 302
11.2.1 Redução de formas 308
11.2.2 Quantidade de representações 312
11.2.3 Número de classe 314
11.2.4 O grupo de classes 316
11.3 Formas quadráticas ternárias 321
11.3.1 Aplicação: soma de três quadrados 323

12 Formas Modulares, Grupo Modular **331**
12.1 O grupo modular 331
12.2 Formas Quadráticas Binárias Definidas 337
12.3 Formas quadráticas indefinidas 339

13 Corpos Quadráticos **341**
13.1 Extensões de Corpos 341
13.2 Corpos Quadráticos 343
13.3 Divisibilidade 348
13.4 Corpos quadráticos e formas quadráticas 350

14 Partições de um Inteiro **351**
14.1 Funções geradoras 351
14.2 Partições 352
14.3 Crescimento de $p(n)$ 355
14.4 Exercícios 355

15 Frações Contínuas **357**
15.1 Frações Contínuas Finitas e Números Racionais 357
15.2 Frações Contínuas Infinitas e Números Irracionais 362
15.2.1 Convergentes 364
15.3 Melhor aproximação 368
15.4 Frações Contínuas Periódicas 371
15.5 Construção de $\mathbb{R}$ com frações contínuas 374
15.6 e é irracional 376
15.6.1 Demonstração de Cohn, com frações contínuas 377
15.6.2 Demonstração de Fourier, sem frações contínuas 379
15.7 π é irracional 381
15.8 ϕ é irracional 383
15.9 Exercícios 385

16 Régua e compasso: o corpo dos números construtíveis **389**
16.1 Números construtíveis 390
16.2 Todos os números construtíveis 397
16.3 Alguns problemas impossíveis 398

Apêndices **400**

A Dicas e Respostas **403**

Sobre este texto

Este texto é uma primeira introdução à Teoria de Números, em duas partes. A primeira segue linearmente, com capítulos dependendo de todos os anteriores; a segunda parte é uma exploração por diferentes caminhos. Cabem aqui alguns comentários.

Requisitos. Presume-se de quem o lê alguma familiaridade com demonstrações, especialmente por indução e também familiaridade com o conceito de número complexo. A partir do Capítulo 13, há a necessidade de rudimentos de Álgebra Linear.

Contexto. O texto é também uma tentativa de contextualizar as técnicas e conceitos apresentados, além de reconhecer a Matemática como processo histórico. Isso é feito através de comentários históricos em notas de rodapé, e muitas vezes através da exposição de caminhos alternativos, que ilustram diferentes qualidades de definições ou demonstrações distintas, ou mesmo a troca de trechos em uma demonstração. Em momentos há discussão sobre as qualidades de demonstrações (transparência, profundidade, possibilidade de generalização) – isto é feito explicitamente, por exemplo, na apresentação de quatro demonstrações diferentes da lei da reciprocidade quadrática. Além de contextualizar as técnicas, ficará clara a intenção de jogar luz, ainda que de forma limitada, sobre o processo histórico que moveu a Matemática que é hoje conhecida, deixando claros os vieses culturais e seus efeitos. Diversos conceitos, teoremas e técnicas recebem nomes de personagens que (na maioria das vezes[2]) de fato os trabalharam ou introduziram em algum contexto, mas não necessariamente são os primeiros a fazê-lo – há uma quantidade importante de "arte prévia" fora da Europa (em particular, no mundo Árabe, na China e na Índia).

Complexos. Os números complexos estão presentes desde cedo no texto, refletindo a importancia que estes tem na Matemática[3] (estão incluídas dis-

[2] Em alguns casos nem isso, como na história da equação de Pell.

[3] Uma longa estrada foi percorrida. No Capítulo 12 de

Kleiner, Israel. **Excursions in the History of Mathematics**. [*S. l.*]: Birkhauser, 2012.

Kleiner conta a história do desenvolvimento dos números complexos: Bhaskara teria escrito

> *O quadrado de um número positivo, também o de um número negativo, é positivo; e a raiz quadrada de um número positivo é dupla, positiva e negativa;*

cussões sobre inteiros Gaussianos, raízes da unidade, a demonstração da lei da reciprocidade quadrática usando raízes da unidade – dada por Gauss –, e formas modulares).

Apresentação moderna. Estruturas algébricas e outros conceitos são apresentados tão cedo quando possível no texto, de maneira a tornar transparente a forma como a teoria de Números está integrada com outras áreas da Matemática, e também refletindo uma visão moderna do assunto. isto *não* é feito de maneira a forçar abstrações abrutamente, e sim gradualmente, muitas vezes alternando conceitos abstratos com exemplos concretos.

Enunciados em notas de rodapé. Não são usadas apenas para contextualização histórica, claro. Além de comentários gerais que não cabem no texto, os teoremas e lemas definidos anteriormente tem seu enunciado reproduzido em notas de rodapé quando são citados. Por exemplo, quando o Teorema de Wilson é usado, a nota de rodapé traz seu enunciado – com isto o leitor iniciante na área, que não se lembre exatamente se o enunciado mencionava "$+1$" ou "-1", poderá resolver sua dúvida na mesma página.

Sistemas de escrita e transliterações. Os nomes de autores estrangeiros, quando em notas de rodapé, são apresentados em seus sistemas de escrita nativos, e também transliterados. Para o Chinês, tanto o sistema simplificado como o tradicional são usados, e a pontuação européia (sinais como ":" e "?") também – estas marcas não existiam em textos clássicos, mas foram incorporadas à escrita chinesa nos Séculos XIX e XX. Em Latim e Alemão, há uma tentativa e manter as letras não mais usadas, como o esse longo (ſ)[4] e o "eszett" (ß)[5] – mas devido à complexidade de manter um documento LaTeX multilíngue com ligaduras, não houve esforço para preservá-las.

---

não há raiz quadrada de um número negativo, porque um número negativo não é um quadrado.

Somente em 1545 é que Cardano, em seu livro Ars Magna (A Grande Arte) considerou manter raízes quadradas negativas em suas contas, percebendo que isto era útil (em ocasiões, as raízes negativas se cancelavam, e Cardano chegava a um resultado sem elas).

> *Se alguém te disser, divida 10 em duas partes, tais que uma das quais multiplicada pela outra produza... 40, é evidente que neste caso a questão é impossível. Ainda assim, deveremos resolver o problema.*

O problema equivale a resolver $x+y = 10$ e $xy = 40$. Cardano aplicou seu método (completando quadrados) e obteve os números $5 + \sqrt{-15}$ e $5 - \sqrt{-15}$. Formalmente multiplicou os dois e obteve 40, mas ainda assim considerou o resultado "inútil". Ainda assim, fo a primeira vez que uma raiz negativa foi formalmente apresentada como solução de um problema. Logo depois, Bombelli passou a usar operações com raízes negativas, embora ainda fossem necessários alguns séculos para que os matemáticos aceitassem os números complexos.

[4] Esta é a origem do símbolo de integral ($\int$).

[5] Em Alemão, o eszett teve seu uso diminuído após uma reforma ortográfica em 1996, mas ainda é usado.

Nomenclatura

Neste texto usamos marcadores para final de definições (⧫), exemplos (◀) e demonstrações (□). Em alguns Capítulos, vetores são denotados por variáveis em negrito (por exemplo, "$\mathbf{v}$").

(a, b, c) forma quadrática binária $ax^2 + bxy + cy^2$, página 302

$*$ composição de formas quadráticas, página 318

$*$ convolução de Dirichlet, página 212

$[E : F]$ grau extensão E sobre F, página 342

$[x_0; x_1, x_2, \ldots, x_n]$ Fração contínua $x_0 + 1/(x_1 + 1/(x_2 + \cdots + 1/(x_n)))$, página 359

$\lceil x \rceil$ função menor inteiro $\geq x$ (teto de x), página 224

$\overline{\alpha}$ conjugado complexo de α., página 83

$\overline{\alpha}$ conjugado em corpo quadrático, página 344

Δ discriminante de forma quadrática, página 303

δn função $delta$ de Kronecker (1 sse $n = 1$, senão zero), página 200

$\mathrm{Disc}(p)$ Discriminante de polinômio (def. em nota de rodapé), página 298

$\lfloor x \rfloor, [x]$ função maior inteiro $\leq x$ (chão de x), página 224

Γ grupo modular, página 332

$\mathbb{Z}$ conjunto dos números inteiros, página 30

$\mathbb{Z}/n\mathbb{Z}$ Anel dos inteiros módulo n, página 121

$\mathbb{Z}[\omega]$ inteiros quadráticos, página 347

$\mathbb{Z}_n$ Anel dos inteiros módulo n, página 121

$\lambda(\cdot)$ Norma em domínio euclideano, página 85

$\Lambda(x)$ função de Mangoldt, página 222

$\left(\frac{a}{m}\right)$ Símbolo de Jacobi, página 243

$\left(\frac{a}{p}\right)$ Símbolo de Legendre, página 243

$\lfloor x \rceil$ Inteiro mais próximo de x, página 85

$\mathbb{1}$ função constante um, página 201

$\mathrm{mdc}\,(a, b)$ máximo divisor comum de a e b, página 60

$\mathrm{mmc}(a, b)$ mínimo múltiplo comum de a e b, página 70

$\mu(n)$ função μ de Moebius, página 214

$\mathbb{N}$ conjunto dos números naturais, página 7

ω $\sqrt{d}$ ou $(1 + \sqrt{d})/2$ (conveniência de notação para inteiros quadráticos), página 347

$\mathrm{ord}_p(n)$ ordem de p em n, página 96

ϕ razão áurea, página 74

$\phi(n)$ quantidade de co-primos com n, menores ou iguais a n, página 169

$\phi(n)$ quantidade de co-primos com n, menores ou iguais a n, página 201

$\pi(n)$ quantidade de primos menores ou iguais a n, página 229

$\mathcal{O}_F$ anel de inteiros quadráticos, página 348

$\mathcal{O}_F$ grupo de unidades de inteiros quadráticos, página 349

Q_n resíduos quadráticos módulo n, página 241

$\mathrm{rad}\, n$ radical do número n, página 235

$\mathbb{Q}$ conjunto dos números racionais, página 30

$\mathbb{Q}[\sqrt{d}]$ corpo quadrático, página 343

$\mathbb{R}[x]$ anel de polinômios em uma variável real, página 35

$\mathbb{R}_{\mathtt{trop}}$ corpo dos números tropicais, página 38

$\sigma(n)$ soma dos divisores de n, página 201

$\sim$ equivalência de formas quadráticas, página 301

$\sim$ equivalência de pontos em $\mathbb{H}$, página 333

$\mathrm{Tr}(\alpha)$ traço de elemento em corpo quadrático, página 344

$\mathbb{H}$ meio-plano superior, página 333

U_n grupo de unidades módulo n, página 187

ζ raiz primitiva da unidade, página 192

$a \equiv b \pmod{m}$ a é congruente a b módulo m, página 120

$a \mid b$ a divide b, página 57

$a \nmid b$ a não divide b, página 57

$a^{(i)}$ i-ésimo convergente de irracional aproximado por fração contínua, página 364

$c(p)$ conteúdo de um polinômio p, página 113

$d(n)$ número de divisores de n, página 201

$f \equiv g$ o polinômio f é equivalente a g, página 156

$f \sim g$ o polinômio f é congruente a g, página 156

F_n número de Fermat, página 101

g_k soma de Gauss, página 261

$GL(n, F)$ grupo linear geral, página 332

$h(\Delta)$ número de classe do discriminante fundamental Δ, página 314

$k(m)$ período de sequência da Fibonacci módulo m, página 161

$LR_m(x)$ menor resíduo congruente a x módulo m, página 254

$M(N)$ função de Merten, página 238

M_p número de Mersenne, página 98

$N(n)$ quantidade de soluções da congruência $a^2 \equiv -1 \pmod{n}$, página 286

$N(z)$ norma do inteiro Gaussiano z, página 81

$n\#$ primorial de n, página 102

$P(n)$ quantidade de representações próprias de n com $x > 0$, página 286

$p(n)$ quantidade de partições de um inteiro, página 353

p_i/q_i i-ésimo convergente de irracional aproximado por fração contínua, página 364

$R(n)$ quantidade de representações de n, página 286

$r(n)$ quantidade de representações próprias de n, página 286

$R[[x]]$ anel das séries formais de potências na variável x, sobre o anel R, página 352

$R_{n\times n}$ matriz de Redheffer de ordem n, página 239

$s(n)$ sucessor de número natural, página 7

$SL(n, F)$ grupo linear especial, página 332

$u(\mathrm{mod}\, m)$ sequência de Fibonacci módulo m, página 160

u_n n-ésimo número de Fibonacci, página 73

$w(f)$ quantidade de automorfismos da forma quadrática f, página 312

Parte NVLLA

Capítulo 1

Introdução

O objeto de estudo da Teoria dos Números é o conjunto dos números inteiros, $\ldots, -2, -1, 0, +1, +2, \ldots$, e suas propriedades[1].
Como exemplo elementar, sabemos que um número escrito na base dez é divisível por dois quando seu último dígito é par; e que é divisível por cinco quando seu último dígito é zero ou cinco. Estas duas propriedades podem ser *demonstradas* sem grande dificuldade, embora demonstrações fáceis não sejam regra.
Muito do desenvolvimento da Teoria dos Números se dá a partir de *observações*: somente após observar em experimentos que há uma grande quantidade de números primos, perfeitos, de ternos Pitagóricos, e outros objetos, Matemáticos decidiram por conjecturar suas propriedades. Assim, embora muito do texto a seguir seja devotado a enunciar e demonstrar fatos sobre números, deve-se ter em mente que muitas das Definições e Teoremas que estudamos são fruto de longo e extenso trabalho de observação. Muito desse trabalho empírico foi realizado quando não havia computadores ou calculadoras – mas com a existência destes, a dificuldade deixa de ser o poder computacional para fazer observações, e sim a intuição para decidir *o que observar*.
É muito comum que enunciados sobre números inteiros sejam de muitíssimo simples expressão, passando a ilusão de que sua demonstração é, também, simples – e o oposto acontece! O conhecido Último Teorema de Fermat, por exemplo, afirma que para n inteiro maior que dois, a equação $x^n + y^n = z^n$ não tem soluções com $x \neq 0$. Esta afirmação foi feita sem demonstração[2]

[1] Também de números não inteiros, quando há relação entre eles e os inteiros.

[2] Fermat tinha um exemplar do *Diophantus* (coleção de tratados por Diofanto de Alexandria), onde um exercício propunha "decompor um quadrado em uma soma de dois quadrados". Na margem do livro, Fermat apontou que *"No entanto, é impossível separar um cubo em cubos, ou uma quarta potência em quartas potências, ou, em geral, uma potência maior que dois em potências similares. Eu descobri uma prova maravilhosa disso, que esta margem é demasiado pequena para comportar"*. Dada a complexidade da demonstração que temos hoje, é crença

por Pierre de Fermat em 1637, e permaneceu sem demonstração até 1994, quando Andrew Wiles conseguiu finalmente – usando um ferramental matemático longe de ser trivial – garantir que de fato a proposição é verdadeira.

comum entre Matemáticos que a demonstração de Fermat tivesse alguma falha sutil. Fermat usualmente trocava cartas com outros matemáticos, e esta nota não estava em qualquer de suas cartas – ela foi encontrada na margem de um livro, onde havia muitas outras anotações, portanto um "lembrete para si mesmo". Isso pode indicar também que Fermat poderia ter tido uma idéia que anotou, mas que posteriormente verificou que era falha (e por isso nunca chegou a apresentá-la a outros).

Capítulo 2

Números

Este Capítulo passa por uma carcterização de números naturais (não é uma *definição*, apenas uma "caracterização" – ums descrição de propriedades desses números). Esta abordagem foi escolhida porque leva naturalmente à descrição da indução finita como método de demonstração. No entanto, esta visão, com números sento definidos de forma abstrata, é recente na História da Matemática. O conceito de número surgiu muito antes desta formalização, e as definições/construções anteriores não são "erradas". São diferentes. Escolhemos uma visão por sua utilidade, não por uma suposta superioridade.

Para se demonstrar o que quer que seja, precisamos partir de pressupostos anteriores. Tomando um exemplo qualquer dentro da Matemática: quando nosso foco de atenção é o Cálculo, demonstramos que a regra da cadeia para derivação é válida – mas aquela demonstração presume como certo que as operações que usamos ao demonstrar são bem definidas e que suas propriedades valem. É interessante lançar o olhar sobre estas operações e questionar *o que estamos presumindo*. Levando este raciocínio adiante, chegamos ao estudo de conjuntos de números e operações sobre eles, a que damos o nome de "estruturas algébricas". Um passo mais e podemos questionar se há alguma forma de definir rigorosamente o que chamamos de "números naturais" (e inteiros, racionais, e reais). É evidente que em algum momento teremos de parar e nos contentar em aceitar alguma quantidade de fatos e entidades fundamentais, de forma a poder trabalhar as demonstrações que precisamos. A estes fatos fundamentais damos o nome de *axiomas*[1].

Neste Capítulo abordamos os *Axiomas de Dedekind-Peano*, que definem o

[1] O que se toma como axioma e o que se define e demonstra varia conforme o objetivo. Em um curso de Cálculo aplicado, pode-se definir os números reais axiomaticamente, apresentando suas propriedades apenas. Já em outros cursos é interessante mostrar que é possível definir os reais e as operações sobre eles a partir dos racionais.

conjunto dos números naturais. A partir destes, é possível desenvolver tanto as operações aritméticas básicas em $\mathbb{N}$ como os conjuntos $\mathbb{Z}$, $\mathbb{Q}$ e, após desenvolver um ferramental mais elaborado, construir o conjunto dos reais e operações aritméticas nele.

2.1 Naturais

Os *Axiomas de Dedekind-Peano*, descritos[2] por Dedekind[6] e Peano[7], são uma maneira de definir os números naturais usando tres conceitos primitivos ("número", "zero" e "sucessor") e cinco axiomas. Aqui reproduzimos os Axiomas de Dedekind-Peano que nos interessam (há quatro deles que tratam da relação de igualdade, mas presumimos aqui que esta já está bem definida[8]). Este recorte é comum na apresentação destes axiomas.

[2] No século XIX é que ganha força o interesse em axiomatizar a aritmética como fundamento da Matemática. Há publicações de axiomatizações da aritmética de números naturais em 1881 (de Charles Sanders Pierce[3]), e 1888, de Richard Dedekind.

Pierce, Charles Sanders. On the Logic of Number. **American Journal of Mathematics**, v. 4, n. 1, p. 85–95, 1881.

Dedekind, Richard. **Was sind und was sollen die Zahlen?** [*S. l.*], 1888. Publicado como brochura.

Giuseppe Peano publicou uma versão simplificada dos axiomas de Dedekind, mas ainda enumerando nove axiomas (e não cinco, como fazemos hoje).

Peano, Giuseppe. **Arithmetices principia, nova methodo exposita**. [*S. l.*], 1889. Disponível em Latim, com tradução para Inglês em `https://github.com/mdnahas/Peano_Book`.

Este idéia ganhou força, e houve muito interesse de Matemáticos no início do Século XX em uma possível formalização completa da Matemática. Um dos expoentes dessa visão foi Russel[4], e a essa escola de pensamento se dá o nome de *Logicismo*. Há um livro inrodutório do próprio Russel sobre o assunto.

Russel, Bertrand. **Introdução à Filosofia Matemática**. [*S. l.*]: Zahar, 1974.

O plano de formalizar completamente a Matemática, no entanto, sofreu um duro revés com a publicação dos trabalhos de Gödel[5], que mostravam essencialmente que o objetivo era impossível.
Havendo interesse, o livro de Eliott Mendelson trata de Lógica Formal, tendo inclusive um capítulo sobre Teoria Formal de Números.

Mendelson, Eliott. **Introduction to Mathematical Logic**. 6. ed. [*S. l.*]: CRC Press, 2015.

A Lógica Formal, da maneira como é tratada por Mendelson, no entanto, já é posicionada um tanto distante da Matemática e dos matemáticos.
No final do século XX e início do século XXI, houve uma renovação da idéia de formalização da Matemática (que nunca desapareceu, mas teve um período de pouca força), desta vez com o surgimento dos *assistentes de prova* – sistemas de software que permitem ao matemático verificar formalmente suas demonstrações (e eventualmente realizam partes delas de forma automática). Isto, no entanto, requer um esforço do matemático para codificar a demonstração na linguagem do software.

[6] Richard Dedekind (1831-1916), Alemão.

[7] Giuseppe Peano (1858-1932), Italiano.

[8] Na formulação original de Peano, havia mais quatro axiomas, que descrevem as propriedades da igualdade (deterinavam que a igualdade é reflexiva, simétrica, transitiva, e que se x

(i) 0 é um número natural[9];

(ii) se n é um número natural, então o *sucessor de* n, denotado $s(n)$, é um número natural;

(iii) 0 não é sucessor de qualquer outro número natural;

(iv) se dois naturais p e q tem o mesmo sucessor, então p e q são iguais;

(v) se (i) 0 pertence a um conjunto X; e (ii) se sempre que $n \in X$ implicar que $s(n)$ também pertença a X – então X é exatamente o conjunto dos naturais.

O quinto axioma de Dedekind-Peano expressa o *princípio da indução finita*. Denotaremos o conjunto dos número naturais por $\mathbb{N}$. No entanto... Não mostramos que eles existem! Somente definimos "como" devem ser.

2.1.1 Um modelo para $\mathbb{N}$

Os axiomas de Dedekind-Peano são uma *definição* do conjunto dos números naturais. Esta definição somente nos informa as propriedades que os naturais devem ter – mas não nos ajuda a construir um objeto que tenha essas propriedades. Se conseguirmos construir um conjunto que obedeça os axiomas de Dedekind-Peano, teremos construído um *modelo* para os números naturais.

Como parte do esforço de formalizar a Teoria dos Conjuntos como fundamento da Matemática, Zermelo[10], Fraenkel[11] e Skolem[12] desenvolveram[13] o que se chama hoje de Teoria de Conjuntos de Zermelo-Fraenkel (chamada de ZF, ou ZFC quando inclui o Axioma da Escolha[14]). A partir da Teoria

é natural e $x = y$ então y também é natural), mas estes não são incluidos em apresentações modernas, onde a igualdade é tratada como conceito primitivo.

[9] A formulação original de Dedekind-Peano não incluia o zero como natural, e definia os naturais como $\{1, 2, \ldots\}$. É comum incluir o zero por ser o elemento neutro para a adição.

[10] Ernst Zermelo (1871-1953), Alemão.

[11] Abraham Fraenkel (1891-1965), Alemão-Ieraelita.

[12] Thoralf Skolem (1887-1963), Norueguês.

[13] Não juntos – Zermelo publicou seu trabalho inicialmente em 1908; Fraenkel e Skolem independentemente o modificaram em 1922.

Zermello, Ernst. Investigations in the foundations of set theory. *In:* **Heijenoort**, Jean van (ed.). **From Frege to Gödel: A Source Book in Mathematical Logic, 1879 − 1931**. [*S. l.*]: Harvard University Press. p. 199–215.

Bernays, Paul; **Fraenkel**, Abraham. **Axiomatic Set Theory**. [*S. l.*]: North-Holland, 1958.

Na introdução, Fraenkel dá uma visão de como era originalmente o sistema Zermello-Fraenkel.

Skolem, Thoralf. Some Remarks on Axiomatized Set Theory. *In:* **Heijenoort**, Jean van (ed.). **Harvard University Press**. [*S. l.*]: Harvard University Press. p. 290–301.

[14] O Axioma da Escolha diz que "dada uma coleção de conjuntos não vazios, pode-se *escolher* um elemento de cada conjunto da coleção". Há uma grande quantidade de enunciados equivalentes a este – por exemplo "todo espaço vetorial sobre um corpo tem uma base".

ZF houve várias construções do conjunto dos naturais. Um destes modelos, dado por John von Neumann, é apresentado aqui. Usamos apenas a existência do conjunto vazio e a operação de união. Determinamos que

$$\begin{aligned} &\text{o número } 0 \text{ é} && \emptyset \\ &\text{o número } 1 \text{ é} && \{0\} = \{\emptyset\} \\ &\text{o número } 2 \text{ é} && \{0,1\} = \{\emptyset, \{\emptyset\}\} \\ & && \vdots \end{aligned}$$

Observe que estamos naturalmente definindo o sucessor de qualquer número como

$$s(n) = n \cup \{n\},$$

e que o número n é definido como o conjunto de seus antecessores, $n = \{0, 1, 2, \ldots, n-1\}$.
É possível demonstrar que os axiomas de Dedekind-Peano valem para esta construção dos naturais.

2.1.2 Independência dos axiomas

Queremos que nossas definições não incluam mais do que o necessário – um conjunto menor de axiomas é usualmente mais elegante, e exige menos trabalho quando precisamos verificar se algum objeto está de acordo com aqueles axiomas.
Por exemplo, há cinco axiomas da Geometria Euclideana plana:

(i) pode-se traçar uma linha reta entre quaisquer dois pontos;

(ii) qualquer segmento de reta pode ser estendido indefinidamente;

(iii) um círculo pode ser traçado com qualquer ponto como centro e com qualquer raio;

(iv) todos os ângulos retos são iguais;

(v) dado qualquer ponto P fora de uma reta R, é possível traçar uma única reta paralela a R passando por P.

Por séculos, Matemáticos acreditaram que o quinto axioma (chamado de "axioma das paralelas") era desnecessário, e que poderia ser deduzido a partir dos outros – só não conseguiam encontrar a demonstração. No entanto, no século dezenove Lobachevsky– *Никола́й Ива́нович Лобаче́вский* em Russo –[15] e Bolyai[16] mostraram que se o quinto axioma for modificado a

[15] Nikolai Ivanovich Lobachevsky (1792-1856), Russo.
[16] János Bolyai (1802-1860), Húngaro.

Geometria resultante é completamente diferente da Geometria Euclideana. Ao trocar "uma reta paralela a R" por "ao menos duas retas paralelas a R", surgem os Axiomas da *Geometria Hiperbólica*[17].
Ao apresentar modelos diferentes que satisfazem todos os axiomas, exceto um deles, provamos que aquele axioma não pode ser deduzido a partir dos outros.
Os axiomas de Dedekind-Peano são *independentes*: nenhum deles pode ser demonstrado a partir dos outros. Se removermos um deles, teremos algo diferente dos números naturais.

Teorema 2.1. *Os axiomas de Peano são independentes.*

Demonstração. Construimos, para cada um dos cinco axiomas, um *modelo para* $\mathbb{N}$ que satisfaz todos os outros menos ele. Damos cinco destes modelos a seguir.

(i) Para o primeiro axioma, o conjunto vazio. Note que o primeiro axioma é o único que requer a *existencia* de um elemento – os outros são afirmações quantificadas com $\forall$, e portanto condicionais. Assim, para o conjunto vazio todos os outros axiomas são verdadeiros por vacuidade, e $\emptyset$ seria um modelo viável para os naturais;

(ii) Para o segundo axioma, o conjunto $\{0\}$, com $s(0) = 1$;

(iii) Para o terceiro axioma, o conjunto $\{0\}$, com $s(0) = 0$;

(iv) Para o quarto axioma, o conjunto $\{0, 1\}$, sendo que um sucede tanto zero como um: $s(0) = s(1) = 1$;

(v) Para o quinto axioma, podemos incluir mais elementos no conjunto: $\{0, 1/2, 1, 3/2, 2, \ldots\}$, mas mantendo a função sucessor $s(n) = n + 1$. □

2.2 Indução

O quinto Axioma de Dedekind-Peano, chamado de "axioma da indução", é, mais que parte de uma definição, uma poderosa ferramenta para demons-

[17] Gauss declarou ter construído um sistema sem o postulado das paralelas, e o chamou de "Geometria não-Euclideana" – mas não o publicou. Taurinus[18] publicou alguns resultados relacionados, e finalmente um sistema completo de geometria hiperbólica foi publicado independentemente por Lobachevsky– *Никола́й Ива́нович Лобаче́вский* em Russo –[19] e por Bolyai[20]. A história do postulado das paralelas é tratada detalhadamente por David Burton.

Burton, David. The History of Mathematics: An Introduction. *In:* 6. ed. [*S. l.*]: McGraw-Hill, 2006. 11 - Nineteenth-Century Contributions: Lobachevsky to Hilbert.

trações, e é usualmente apresentado como tal[21]. A seguir o axioma é

[21] É um princípio antigo, e há registros de seu uso desde pelo menos 1575. W. H. Bussey afirma que:

> *Cantor em seu Vorlesungen iuber Geschichte der Mathematik diz que Pascal foi quem originou o método da indução completa. Mas corrigiu essa afirmação em uma breve nota no Zeitschrift fur Mathematischen und Naturwissenschaftlichen Unterricht. Nessa nota ele aponta que foi informado por G. Vacca que Maurolycus descreveu e usou o método em sua aritmética, que foi publicada em 1575,*

O original:

> *Cantor in his Vorlesungen iuber Geschichte der Mathematik says that Pascal was the originator of the method of complete induction. But he has corrected this statement in a brief note in the Zeitschrift fur Mathematischen und Naturwissenschaftlichen Unterricht. In this note he says that he has been informed by G. Vacca that Maurolycus described and used the method in his arithmetic which was published in 1575.*

Bussey, W. H. The Origin of Mathematical Induction. **The American Mathematical Monthly**, v. 24, n. 5, p. 199–207, 1917.

O texto de Giovanni Vacca, citado por Bussey, é:

Vacca, Giovanni. Maurolycus, the first discoverer of the principle of mathematical induction. **American Mathematical Society**, v. 16, n. 2, p. 70–73, 1909.

Maurolycus (ou Maurolico, Maurolicu, *Μαυρόλυκος*, 1494-1575) foi um matemático e astrônimo Siciliano. A "aritmética" de Maurolycus, onde o princípio da indução foi apresentado, é

Maurolycus, Franciscus. **Arithmeticorum libri duo**. [*S. l.*], 1575. Incluso na obra "D. Francisci Maurolyci Opuscula mathematica".

Talvez seja razoável presumir que o princípio possa ter surgido também em diferentes contextos, possivelmente antes disso. Por exemplo, a demonstração de Euclides de que "há mais números primos do que qualquer quantidade proposta" não é uma demonstração por indução, da forma como entendemos hoje, mas é um passo de indução perfeitamente aceitável (a partir de um conjunto de primos de tamanho n, determina-se um novo conjunto, de tamanho $n+1$) – a demonstração está na Seção 5.3, com comentários em uma nota de rodapé.

Quanto às demonstrações de Pascal por indução, é interessante observar que eram feitas com muito menos rigor e formalidade que as produzidas a partir do Século XX. Por exemplo em seu "Tratado do Triângulo Aritmético"[22], Pascal define o triângulo aritmético, e enuncia várias "consequências do triângulo" (teoremas a respeito dele).

Pascal, Blaise. **Traite du Triangle Arithmetique, avec quelques autres petits traitez sur la mesme matiere**. Paris: Guillaume Desprez, 1665.

Como exemplo, a oitava consequência, com a demonstração de Pascal, é dada a seguir.

> **Oitava Consequência** *Em todo triângulo aritmético, a soma das células de cada base é um número da progressão dupla que começa com a unidade da qual o expoente é o mesmo que aquele da base.*
>
> *Porque a primeira base é a unidade. A segunda base é o dobro da primeira, portanto é 2. A terceira base é o dobro da segunda portanto é 4.* **E assim até o infinito.**

A expressão "e assim até o infinito" indica que se deve repetir o argumento infinitas vezes, porque ele se aplica repetidamente – o que poderia ser resumido modernamente ao descrever um passo de indução. O original de Pascal:

apresentado novamente, desta vez como técnica e não como definição.
Dado um predicado P a respeito de número naturais, se

(i) $P(0)$ vale;

(ii) para todo natural k, a validade de $P(k)$ implica na validade de $P(s(k))$;

então $P(n)$ vale para qualquer $n \in \mathbb{N}$.
Dizemos que $P(0)$ é a "base"; que $P(k)$ é a "hipótese de indução"; e que demonstrar $P(k) \Rightarrow P(s(k))$ é o "passo de indução".
Nos exemplos que seguem, denotaremos $s(k)$ por $k+1$, para simplificar a notação.

Exemplo 2.1. *Como primeiro exemplo, tome o predicado*

$$P(n) = \text{“}9^n - 2^n \text{ é divisível por } 7\text{”}$$

Começamos com a base, provando que $P(0)$ *vale:*

$$9^0 - 2^0 = 1 - 1 = 0, \text{ divisível por } 7$$

Agora realizamos o passo: provamos que $P(k) \Rightarrow P(k+1)$.
Hipótese: $9^k - 2^k$ *é divisível por* 7 *(esta é* $P(k)$*)*

Consequence huictiesme En tout Triangle Arithmetique, la fomme des cellules de chaque base, est un nombre de la progression double, qui commence par l'unité, dont l'exposant est le mesme que celuy de la base.
Car la premiere base est lunité. La seconde est double de la premiere, donc elle est 2. La troisiesme est double de la seconde, donc elle est 4. **Et ains à linfiny.**

Há uma longa exposição das propriedades do triângulo no texto de Bondarenko:

Bondarenko, Boris. **Generalized Pascal Triangles and Pyramids**. [*S. l.*]: The Fibonacci Association, 1993. Disponível em `https://www.fq.math.ca/pascal.html`.

[22] O triângulo, embora leve o nome de Pascal, era conhecido na China, com o nome de **triângulo de Yáng Hu** (o chinês 杨辉 – Yáng Huī – viveu entre 1238 e 1298, e trabalhou em diversos problemas, incluindo equações quadráticas e quadrados mágicos – mas o triângulo foi registrado em mais de uma ocasião na história da Matemática chinesa, e poderia ter sido descoberto por um antecessor de Yáng Huī , Jiǎ Xiàn (贾宪)); descrito por Omar Khayyam (عمر خيّام, persa, viveu entre 1044 e 1123); e também pelo indiano Halayudha (हलायुध) no século X.

Martzloff, Jean-Claude. **A History of Chinese Mathematics**. [*S. l.*]: Springer, 2006.

Este livro contém uma grande quantidade de referencias a idéias que, apesar de serem usualmente citadas como européias, foram registradas anteriormente na China. Uma figura descrevendo duas versões chinesas do triangulo de Pascal está na página 231.

Kennedy, Evelyn. Omar Khayyam. **The Mathematics Teacher**, v. 59, n. 2, p. 140–142, 1966.

Bag, Amulya Kumar. Binomial theorem in ancient India. **Indian Journal of History of Science**, v. 1, n. 1, p. 68–74, 1966.

Passo:

$$\begin{aligned} 9^{k+1} - 2^{k+1} &= 9(9^k - 2^k) + 2^k(9-2) && \text{(verifique!)} \\ 9^{k+1} - 2^{k+1} &= 9(\underbrace{9^k - 2^k}_{=7n \ (\text{hip.ind.})}) + 2^k(7) \\ &= 9(7n) + 2^k(7) && \text{(aqui usamos a hipótese de indução!)} \\ &= 7(9n + 2^k). \end{aligned}$$

Mostramos portanto que $9^{k+1} - 2^{k+1}$ *é múltiplo de sete,* presumindo que $9^k - 2^k$ também é. *Ou seja, presumimos* $P(k)$ *e concluimos que* $P(k+1)$ *vale (note que a sequência de iguialdades acima expressa que* $9^{k+1} - 2^{k+1}$ *é múltiplo de* 7 *– ou seja, expressa que* $P(k+1)$ *é verdade). Isto completa a demonstração.* ◀

Exemplo 2.2. *Neste exemplo usaremos o princípio da indução de maneira um pouco diferente: provaremos a base para* $n = 1$ *(e não para* $n = 0$*), e teremos provado a validade da propriedade para todo natural* a partir de um.

Os números de Fibonacci[23] *são definidos recursivamente da seguinte maneira*[24].

$$\begin{aligned} u_0 &= 0 \\ u_1 &= 1 \\ u_n &= u_{n-1} + u_{n-2} \end{aligned}$$

Provaremos que, para todo inteiro positivo n,

$$\sum_{i=1}^{n} u_i^2 = u_n u_{n+1}.$$

Começamos com a base:

$$\begin{aligned} u_1^2 &= u_1 u_2 \\ 1^1 &= (1)(1) \end{aligned}$$

Hipótese: $\sum_{i=1}^{k} u_i^2 = u_k u_{k+1}$.

[23] Serão definidos novamente e estudados em mais profundidade no Capítulo 4.

[24] É comum denotar o i-ésimo número de Fibonacci por F_i. No entanto, esta notação já será usada neste texto para números de Fermat.

Passo:

$$\begin{aligned}\sum_{i=1}^{k+1} u_i^2 &= \left(\sum_{i=1}^{k} u_i^2\right) + u_{k+1}^2 \\ &= u_k u_{k+1} + u_{k+1}^2 && \text{(pela hipótese de indução)} \\ &= u_{k_1}(u_k + u_k + 1) \\ &= u_{k+1} u_{k+2}.\end{aligned}$$

Mostramos que a fórmula vale para $k+1$*, usando a hipótese de que vale para* k*. Como também mostramos a base – que a fórmula vale para* 1 *– terminamos a demonstração de que ela vale para todo inteiro positivo.* ◀

O Exemplo 2.3 é na verdade um Teorema que usaremos com alguma frequência[25].

Exemplo 2.3. *Para qualquer número real* $x \neq 1$ *e qualquer número natural* $n \geq 1$*,*

$$\sum_{i=0}^{n-1} x^i = \frac{x^n - 1}{x - 1}.$$

A demonstração é por indução em n*.*

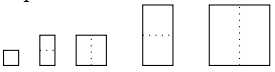
Base: se $n = 1$*, temos*

$$\sum_{i=0}^{1-1} x^i = x^0 = 1 = \frac{x^1 - 1}{x - 1}.$$

[25] Pode ser interessante, em um momento inicial, apresentar intuição geométrica em demonstrações. Este exemplo específico é discutido por Albert B. Bennet em um artigo onde a apresentação visual da série é usada.

Bennet Jr, Albert B. Visualizing the Geometric Series. **The Mathematics Teacher**, v. 82, n. 2, p. 130–136, 1989.

Embora Bennet não tenha apresentado uma *demonstração* geométrica do Teorema, as ilustrações das séries mostradas são bastante interessantes. Para $x = 2$, Bennet apresenta figuras representando valores da série:



$1 \quad 2 \quad 2^2 \quad 2^3 \quad 2^4$

Em seguida, ilustra que a soma dos quatro primeiros termos é $2^4 - 1$:

$1 + 2 + 2^2 + 2^3 \quad = 2^4 - 1$

Agora fazemos o passo de indução. A hipótese é que para n*,*

$$\sum_{i=0}^{n-1} x^i = \frac{x^n - 1}{x - 1}.$$

Então, para $n + 1$*,*

$$\begin{aligned}
\sum_{i=0}^{[n+1]-1} x^i &= \sum_{i=0}^{n} x^i \\
&= x^n + \sum_{i=0}^{n-1} x^i \\
&= x^n + \frac{x^n - 1}{x - 1} && \text{(usamos a hipótese de indução!)} \\
&= \frac{(x-1)x^n + x^n - 1}{x - 1} \\
&= \frac{x^{[n+1]} - 1}{x - 1}.
\end{aligned}$$

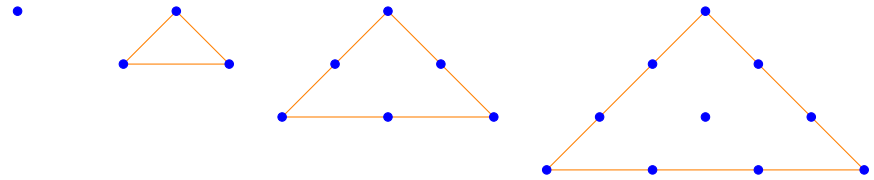
Ou seja,

$$\sum_{i=0}^{[n+1]-1} x^i = \frac{x^{[n+1]} - 1}{x - 1},$$

que é a forma exata da proposição, para $n + 1$*.* ◀

Exemplo 2.4. *Números triangulares*[26] *são números que representam uma quantidade de objetos organizados em um triângulo equilátero. Denotamos o* n*-ésimo número triangular por* T_n*:*

$T_1 = 1$ $T_2 = 3$ $T_3 = 6$ $T_4 = 10$



A partir da figura fica claro que T_n *é igual a* T_{n-1} *com mais uma linha*

[26] Uma interessante exposição é dada por John Hiscocks.

Hiscocks, John. Triangle Numbers in the History of Mathematics. **Teaching Mathematics and its Applications**, v. 9, n. 2, 1990.

Hiscocks comenta a história da representação de números em grades, formando polígonos (algo que remonta a 600 a.c.).
É interessante que o conceito de "número quadrado" é popular, mas o de "número triangular" não (e são a mesma coisa, exceto pela forma escolhida).

contendo n elementos, portanto os números triangulares são

$$T_1 = 1,$$
$$T_n = T_{n-1} + n.$$

Provaremos, por indução em n, que o n-ésimo número triangular é

$$T_n = \frac{n(n+1)}{2}.$$

Base: trivialmente, $n = 1$ é triangular.
Hipótese: $k(k+1)/2$ é o k-ésimo número triangular.
Passo: sabemos que T_k é o k-ésimo número triangular (pela hipótese de indução), e que

$$T_{k+1} = T_k + (k+1).$$

Usamos a hipótese de indução, e

$$\begin{aligned} T_{k+1} &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k(k+1) + 2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2} \\ &= \frac{(k+1)(k+1+1)}{2}, \end{aligned}$$

que a forma do enunciado para $k+1$. ◀

2.2.1 Indução "Forte"

Há uma segunda versão do enunciado do princípio da indução finita, chamado de "indução forte", que pode melhor servir em algumas demonstrações.
Dado um predicado P a respeito de número naturais, se

(i) $P(0)$ vale;

(ii) para todo natural $k < n$, a validade de $P(k)$ implica na validade de $P(n)$;

então $P(n)$ vale para qualquer $n \in \mathbb{N}$.
É usual, ao aplicar esta forma de induçào, usar mais de um caso base – embora tenhamos enunciado a base como "$P(0)$" vale, pode ser necessário provar $P(0)$, $P(1)$ e $P(2)$, por exemplo.
Nos dois exemplos a seguir, provaremos o passo *antes* da base, porque a informação sobre quais casos base serão necessários virá justamente do passo.

Exemplo 2.5. *Provaremos que todo natural maior que onze pode ser escrito como soma de múltiplos de* 4 *e de* 5*.*

A hipótese de indução é: todo natural k *maior ou igual que* 12 *e* ***estritamente menor*** *que* n *pode ser escrito como* $k = 4a + 5b$*, com* $a, b \in \mathbb{N}$*.*

Agora mostramos que isso implica que n *também pode ser escrito dessa forma – ou seja,* $n = 4q + 5r$*.*

O menor dos números que queremos usar é 4*. Tentamos escrever* n*, portanto, usando* $n-4$*: se* $n-4 \geq 12$*, e pela hipótese de indução sabemos como construir* $n-4$*. Só precisamos, portanto, somar mais* 4*. Assim,*

$$\begin{aligned} n &= (n-4)+4 \\ &= 4a + 5b + 4 \\ &= 4(a+1) + 5b. \end{aligned}$$

Mas "$n - 4 \geq 12$*" é o mesmo que* $n \geq 16$*, portanto precisamos dos números entre* 12 *e* 16 *na base. Para a base temos, então:*

$$\begin{aligned} 12 = 4+4+4 &= 3(4) + 0(5) \\ 13 = 5+4+4 &= 2(4) + 1(5) \\ 14 = 5+5+4 &= 1(4) + 2(5) \\ 15 = 5+5+5 &= 0(4) + 3(5). \end{aligned}$$

◀

Exemplo 2.6. *Seja* (a_n) *a sequência*

$$a_n = \begin{cases} a_1 = +1 \\ a_2 = -1 \\ a_n = 2a_{n-1} - a_{n-2} \quad \text{se } n > 2 \end{cases}$$

Provaremos que

$$a_n = 3 - 2n.$$

A hipótese de indução é que, para todo $k \leq n$*,* a_k *tem a forma acima.*

Para o passo, mostraremos que isso implica que a_n *também é dessa forma. A partir da definição de* a_n *obtemos*

$$\begin{aligned} a_n &= 2a_{n-1} - a_{n-2} \\ &= 2(3 - 2(n-1)) - (3 - 2(n-2)) \\ &= 3 - 2n. \end{aligned}$$

Como usanos a_{n-1} *e* a_{n-2} *no passo, precisamos dos dois primeiros termos*

na base. Asism, temos

$$a_1 = 3 - 2(1) = +1$$
$$a_2 = 3 - 2(2) = -1,$$

e a demonstração está completa. ◀

Exemplo 2.7. *Seja* (a_n) *uma sequência de naturais tal que*[27]

$$n \leq \sum_{k=1}^{n} a_k^2 \leq n + 1 + (-1)^n.$$

Provaremos que $a_n = 1$ *para todo* n.
Base: Seja $n = 1$. *Então*

$$1 \leq \sum_{k=1}^{1} a_1^2 \leq 1 + 1 + (-1)^1$$
$$1 \leq a_k^2 \leq 1,$$

o que implica que $a_1 = 1$.
Hipótese de indução: $a_k = 1$ *para* $1 \leq k \leq n$.
Passo: mostraremos que $a_{n+1} = 1$.

$$n + 1 \leq \left(\sum_{k=1}^{n} a_k^2 \right) + a_{n+1}^2 \leq (n+1) + 1 + (-1)^n$$
$$n + 1 \leq n + a_{n+1}^2 \leq (n+1) + 1 + (-1)^{n+1}$$
$$1 \leq +a_{n+1}^2 \leq 1 + 1 + (-1)^{n+1}$$
$$1 \leq +a_{n+1}^2 \leq 2 + (-1)^{n+1}.$$

Então a_{n+1}^2 *é maior ou igual que um, mas também é menor ou igual que* $2+(-1)^{n+1}$, *que pode ser* 1 *ou* 3. *De qulaquer maneira, como é um quadrado, só pode ser um.* ◀

Um exemplo mais intressante de indução forte é o Toerema Fundamental da Aritmética (todo natural pode ser escrito unicamente como produto de primos). O enunciado está no Capítulo 5.

2.2.2 Aritmética

Tendo caracterizado o conjunto dos números naturais, precisamos de operações para que possamos realizar operações com eles. Definimos a seguir

[27] Este problema estava incluído na Hong Kong Advanced Level Examination em 1995.

soma e multiplicação para naturais, a partir somente de nossa construção (usamos somente o conceito de número natural e o de sucessor).

Definição 2.1 (soma e multiplicação en $\mathbb{N}$)**.** *As operações de* ***soma*** *e* ***multiplicação*** *para naturais são:*

$$n + 0 = n$$
$$n + s(m) = s(n + m)$$

$$n0 = 0$$
$$ms(n) = mn + m.$$ ◀

Será útil também dar nome ao número um, para tornar mais confortável algumas demonstrações adiante:

Definição 2.2 (um)**.** $s(0) = 1$. ◀

Não presumimos nada, por mais intuitivo que seja, sem demonstrar – a seguir, por exemplo, provamos que $s(a) = a + 1$.

Lema 2.1. $\forall a \in \mathbb{N}, s(a) = a + 1$.

Demonstração. A demonstração é direta:

$$\begin{aligned} s(a) &= s(a + 0) && \text{(definição de soma)} \\ &= a + s(0) && \text{(definição de soma)} \\ &= a + 1. && \square \end{aligned}$$

Teorema 2.2. *As operações aritméticas que definimos para naturais tem as seguintes propriedades:*

(i) *a soma e a multiplicação são associativas e comutativas;*

(ii) *há elementos neutros únicos* $(0, 1)$ *para soma e multiplicação;*

(iii) *vale a distributividade da multiplicação sobre a soma;*

(iv) *vale o cancelamento tanto para adição como para multiplicação,* $a + c = b + c \Rightarrow a = b$, *e se* $c \neq 0$, $ac = bc \Rightarrow a = b$*;*

(v) $ab = 1 \Rightarrow a = 1$ *e* $b = 1$*;*

(vi) $a + b = 0 \Rightarrow a = b = 0$, *e* $ab = 0 \Rightarrow a = 0$ *ou* $b = 0$*;*

(vii) *o zero aniquila* $\mathbb{N}$*, ou seja,* $\forall n \in \mathbb{N}$, $0n = 0$.

Demonstração. Demonstramos parte das propriedades; outra parte servirá como exercício.

- A soma é associativa, $(a + b) + c = a + (b + c)$. Demonstramos por indução em c. O caso base é com $c = 0$:

$$\begin{aligned} (a + b) + 0 &= a + b && ((\cdots) + 0 = \cdots) \\ &= a + (b + 0) && (b = b + 0) \end{aligned}$$

  Estabelecemos que $(a + b) + 0 = a + (b + 0)$ – ou seja, mostramos que o enunciado vale quando $c = 0$.

  Agora, partimos da hipótese de que a soma é associativa quando fixamos c, ou seja, que $(a + b) + c = a + (b + c)$, e mostramos que isto implica na validade para $s(c)$.

$$\begin{aligned} (a + b) + s(c) &= s((a + b) + c) && \text{(definição de soma)} \\ &= s(a + (b + c)) && \text{(pela hipótese de indução)} \\ &= a + s(b + c) && \text{(definição de soma)} \\ &= a + (b + s(c)) && \text{(definição de soma)} \end{aligned}$$

- A soma é comutativa, $a + b = b + a$. Esta demonstração é um pouco mais longa que a anterior. Primeiro provaremos que $a + 1 = 1 + a$ para todo $a \in \mathbb{N}$, e depois usaremos este fato para provar que $a + b = b + a$.

  Primeira parte, $\forall a \in \mathbb{N}, \quad a + 1 = 1 + a$.
  Base de indução: $a = 0$. Temos $a + 1 = 0 + 1 = 1 + 0 = 1 + a$.

  Hipótese de indução: $a + 1 = 1 + a$

  Passo:

$$\begin{aligned} s(a) + 1 &= s(a) + s(0) && (1 = s(0)) \\ &= s(s(a) + 0) && \text{(definição de soma)} \\ &= s((a + 1) + 0) && \text{(Lema 2.1, } s(a) = a + 1) \\ &= s(a + 1) && \text{(definição de soma)} \\ &= s(1 + a) && \text{(pela hipótese de indução)} \\ &= 1 + s(a) && \text{(definição de soma)} \end{aligned}$$

  Provamos então que $a + 1 = 1 + a$.

  Agora demonstramos que $a + b = b + a$.

  Base: para $b = 1$, é exatamente o que provamos anteriormente ($a+1 = 1 + a$).

  Hipótese de indução: $a + b = b + a$

Passo:

$$\begin{aligned}
a + s(b) &= a + (b + 1) && \text{(Lema 2.1)}\\
&= (a + b) + 1 && \text{(por associatividade)}\\
&= (b + a) + 1 && \text{(pela hipótese de indução)}\\
&= b + (a + 1) && \text{(por associatividade)}\\
&= b + (1 + a) && \text{(pelo caso base, } a + 1 = 1 + a)\\
&= (b + 1) + a && \text{(por associatividade)}\\
&= s(b) + a && \text{(Lema 2.1)}
\end{aligned}$$

- O zero é neutro para adição, como está na própria definição de adição ($n+0 = n$). Por comutatividade, temos também $0+n = n$. Temos ainda que mostrar que zero é o *único* elemento neutro para adição. Suponha que haja outro neutro aditivo, e, ou seja, $a + e = a$ para todo a. Então, para $a = 0$, temos

$$\begin{aligned}
a + e &= a && \text{(por suposição, } e \text{ é neutro)}\\
0 + e &= 0 && \text{(se vale para todo } a\text{, vale para zero)}\\
e + 0 &= 0 && \text{(por comutatividade)}\\
e &= 0. && \text{(definição de soma)}
\end{aligned}$$

  Se $a = 0$, então $e = 0$. Como e é constante (é um número, não uma variável), ele deve sempre ser igual a zero. □

2.2.3 Ordem

Além da aritmética, nos interessa definir alguma relação de ordem em $\mathbb{N}$. Isto pode ser feito de maneira bastante simples, mas não se pode esperar que seja sempre possível em qualquer estrutura (por exemplo, não há como definir para os números complexos uma relação de ordem que seja consistente com as operações aritméticas[28]).

Definição 2.3 (menor ou igual)**.** *Definimos a relação $\leq$ (**menor ou igual**) para naturais de forma que $a \leq b$ se e somente se existe algum $m \in \mathbb{N}$ tal que $a + m = b$.* ◀

Damos exemplos: $4 \leq 10$ porque $4 + 6 = 10$; também $0 \leq 2$ porque $0 + 2 = 2$. Vale observar que esta definição de $\leq$ depende da definição de soma – e que nossa noção de ordem, portanto, está fundamentada na operação que desenvolvemos para os naturais, e só faz sentido a partir dela.

[28] Embora possamos ordenar os complexos, por exemplo, por norma, não podemos escolher uma ordem que os torne um *corpo ordenado*. Se houvesse uma relação de ordem total $\prec$ para $\mathbb{C}$, teríamos necessariamente que $i \prec 0$ ou que $0 \prec i$, mas não ambos. No entanto, nos dois casos chegaríamos a contradições.

Definição 2.4 (relação de ordem parcial)**.** *Uma relação* R *em um conjunto* X *é dita* de ordem parcial não-estrita *se para todos* $x, y, z \in X$*,*

i) R *é reflexiva (*xRx*);*

ii) R *é antisimétrica (*xRy *e* yRx *implicam em* $x = y$*);*

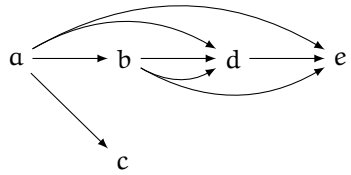
iii) R *é transitiva (*xRy *e* yRz *implicam em* xRz*).*

◀

Exemplo 2.8. *Seja* $X = \{a, b, c, d, e\}$*, e seja* $\prec$ *uma relação em* X *tal que*

$$\begin{array}{lll} a \prec a & a \prec b & b \prec d \\ b \prec b & a \prec c & b \prec e \\ c \prec c & a \prec d & d \prec e \\ d \prec d & a \prec e & \\ e \prec e & & \end{array}$$

O grafo a seguir (chamado de diagrama de Hasse*) representa a relação (uma aresta de* x *a* y *significa que* $x \prec y$*). Para maior clareza, não são mostrados no grafo o relacionamento de elementos com eles mesmos (*$a \prec a$*,* $b \prec b$*) etc.*



Então $\prec$ *é uma relação de ordem parcial não-estrita em* X*, porque* $\prec$ *é:*

- *reflexiva, porque todo elemento se relaciona com ele mesmo (vide primeira coluna na descrição da relação);*
- *antissimétrica, porque só vale* $x \prec y$ *e* $y \prec x$ *quando* $x = y$*;*
- *transitiva, porque sempre que* $x \prec y$ *e* $y \prec z$*, também vale* $x \prec z$*.*

Há elementos que não são comparáveis: c *só é comparável com* a *(*$a \prec c$*), mas não com os outros elementos. Se todos os elementos fossem comparáveis entre si, a relação seria de* ordem total*.* ◀

Exemplo 2.9. *Seja* X *um conjunto, e* $P(X)$ *o conjunto das partes de* X*. Então* $\subseteq$ *é uma relação de ordem parcial não-estrita em* $P(X)$*.*
Verificamos, sem entrar em muitos detalhes: para todos os conjuntos $A, B, C \in P(X)$*,*

i) Reflexividade: $A \subseteq A$*, trivialmente.*

ii) Anti-simetria: $A \subseteq B$ *e* $B \subseteq A$ *implica em* $A = B$*.*

iii) Transitividade: $A \subseteq B$ *e* $B \subseteq C$ *implica em* $A \subseteq C$*.* ◀

Teorema 2.3. $\leq$ *é uma relação de ordem parcial não estrita em* $\mathbb{N}$*.*

A seguir enunciamos o *princípio da boa ordem*, que afirma haver um menor elemento em qualquer subconjunto dos naturais.

Princípio da boa ordem: *Todo subconjunto não vazio dos naturais tem um menor elemento – ou seja, se* $S \in \mathbb{N}$*, então existe um* n *tal que* $\forall q \in S, n \leq q$*.*

É importante notar que a relação que usamos é $\leq$, portanto o "menor" elemento é x aquele que é $x \leq y$ para todo y no conjunto.
Os dois teoremas a seguir constituem o que usualmente se chama de "equivalência dos princípios da indução e da boa ordem". Isso normalmente é feito provando que um dos princípios pode ser deduzido a partir do outro, e que o conjunto resultante de axiomas (Peano (i)-(iv) mais indução; e Peano (i)-(iv) mais boa ordem) definem os mesmo objetos (que neste caso seriam apenas o conjunto $\mathbb{N}$). No entanto, como fica claro no enunciado (e na demonstração) do segundo teorema, o princípio da boa ordem, por si apenas, não implica no princípio da indução. Na verdade, o que se pode demonstrar é que "o princípio da indução é equivalente ao princípio da boa ordem junto com a presunção de que todo natural tem um predecessor único". Se não presumirmos que cada elemento tem um predecessor único, então é possível construir um modelo para (Peano (i)-(iv) mais boa ordem) que é diferente dos naturais – mas a apresentação deste não é adequada para este texto[29]. Mesmo sem verificar a construção explícita do modelo diferente de $\mathbb{N}$ para (Peano (i)-(iv) mais boa ordem), é interessante olhar atentamente o enunciado dos axiomas (i)-(iv): não é possível, deles, concluuir a existência de predecessor para todo natural, e o princípio da boa ordem também não o permite. O da indução, sim.

Teorema 2.4. *O princípio da indução (quinto axioma de Dedekind-Peano) implica no princípio da boa ordem.*

Demonstração. Demonstramos o princípio da boa ordem usando indução. Aqui usamos o princípio da indução forte. Como este é equivalente ao da indução fraca, o resultado não é afetado.

[29] Havendo interesse, o modelo é o conjunto dos ordinais até $\omega + \omega$, cuja definição pode ser verificada em textos sobre Teoria de Conjuntos. Uma discussão da usual confusão nas demonstrações de equivalência dos princípios da boa ordem e da indução está no artigo

Öhman, Lars-Daniel. Are Induction and Well-Ordering Equivalent? **The Mathematical Intelligencer**, v. 41, n. 3, p. 33–40, 2019.

Antes de mais nada, observamos que como 0 não é sucessor de ninguém, não existem números $a, b \neq 0$ tal que $a + b = 0$. Logo ninguém é menor que zero.
Suponha agora que haja algum $S \in \mathbb{N}$ onde não exista menor elemento. Provaremos, por indução, que S é vazio.
Base: necessariamente $0 \notin S$, porque se 0 estivesse em S, ele seria o menor elemento de S (pelo Axioma (iii) de Dedekind-Peano).
Hipótese: supomos que nenhum $k \leq n$ está em S (n também está fora de S).
Passo: $s(n)$ também não pode estar em S, porque pela hipótese de indução não há ninguém menor que $s(n)$ em S, e portanto $s(n)$ seria o menor elemento de S.
Assim, S não tem elementos[30]. □

Teorema 2.5. *Se vale o princípio da boa ordem,* ***e se for verdade que todo número diferente de zero tem um predecessor único****, então vale o princípio da indução (quinto axioma de Dedekind-Peano).*

Demonstração. Presuma que vale o princípio da boa ordem, e presuma também que todo número natural diferente de zero tem um predecessor único – ou seja: se $n \neq 0$ e n é natural, então existe um único k natural tal que $s(k) = n$. Para simplificar a notação, denotaremos o predecessor de n por "$n - 1$". Provaremos que deve valer o princípio da indução finita.
Suponha que uma proposição P valha para zero, e que sempre que vale para n, também vale para $n + 1$. Se o princípio da indução finita vale, isto significaria que $P(k)$ vale para todo natural k – mas *presumimos que não vale o princípio da indução*, e portanto deve existir pelo menos um k tal que $P(k)$ não vale.
Seja $S \subseteq \mathbb{N}$ o conjunto de naturais para os quais P *não* vale. *Pelo princípio da boa ordem*, S tem um menor elemento, que chamamos de k. Logo, $P(k)$ não vale. Como k é o menor elemento de S, e $k - 1 < k$, então $P(k - 1)$ vale. Mas se $P(k - 1)$ vale, então $P(k - 1 + 1) = P(k)$ deve valer. Como mostramos que $P(k)$ deve valer e que também não deve valer, chegamos a uma contradição, e negamos a suposição que fizemos de que deve haver algum k tal que $P(k)$ não vale. Demonstramos portanto o princípio da indução finita usando o princípio da boa ordem. □

Como o quinto axioma é equivalente ao da boa ordem (mais a existência de predecessor), poderíamos reescrever os axiomas de Dedekind-Peano usando como quinto axioma o da boa ordem, e como sexto o da existência de predecessor, descartando o da indução, e o efeito seria o mesmo. No entanto, o princípio da boa ordem depende da relação de ordem, que por sua

[30] Fomos cuidadosos ao enunciar o princípio da boa ordem, falando de subconjunto **"não vazio"** dos naturais!

vez depende da definição de operações aritméticas, que tornariam a descrição dos naturais demasiado grande – é portanto mais interessante manter o axioma da indução.

2.3 Descida Infinita

Uma vez que o princípio da indução dá origem a uma técnica de demonstração, é natural questionar se o princípio da boa ordem também não teria a mesma consequência. Ocorre que o princípio da boa ordem é usado com grande frequência em demonstrações, e foi formalizado por Pierre de Fermat, com o nome de "método (ou princípio) da descida infinita"[31].

[31] W. H. Bussey comenta:

> *A indução matemática foi inicialmente popularizada por Pascal, apesar de ter sido inventada por Maurolycus e usada em sua aritmética, publicada em 1575. É um método de ascenção infinita a partir de um caso especial, no qual o teorema a ser demonstrado precisa ser verificado por argumentação de* n *para* $n+1$*. O método da descida infinita, inventado por Fermat, não é tão amplamente conhecido. A descrição do próprio Fermat pode ser encontrada em uma carta com o título "Relation des nouvelles decouvertes en la science des nombres" que ele escreveu a Pierre de Carcavi em 1659. Nesta carta ele diz a Carcavi que descobriu um novo método para demonstração, e o aplicou com sucesso na resolução de um número considerável de problemas na teoria dos números. Ele chamou o método de descida infinita, ou ilimitada (descente infinie ou indéfinie) . . ..*

O original:

> *Mathematical induction was first brought into prominence by Pascal, although it was invented by Maurolycus and used in his arithmetic which was published in 1575. It is a method of infinite ascent from a special case, for which the theorem to be proved is verified by means of the argument from* n *to* $n+1$*. The method of infinite descent, which was invented by Fermat, is not so widely known. Fermat's own account of it is to be found in a letter entitled "Relation des nouvelles decouvertes en la science des nombres" which he wrote to Pierre de Carcavi in 1659. In this letter he tells Carcavi that he has discovered a new method of demonstration and applied it successfully to the solution of a considerable number of problems in the theory of numbers. He calls it the method of infinite or unlimited descent (descente infinie ou indéfinie) . . .*

Bussey, W. H. Fermat's Method of Infinite Descent. **The American Mathematical Monthly**, v. 25, n. 8, p. 333–337, 1918.

Apesar de Fermat ter declarado ser o inventor do método, este parece ter sido usado já nos Elementos, de Euclides, na demonstração da proposição 31 do livro sete:

> *Todo número composto é medido por um número primo.*

Em Grego,

> *Απας σύνθεντος ἀριθμὸς ὑπὸ πρώτου τινὸς ἀριθμοῦ μετρεῖται.*
> *(Apas sýnthentos arithmós ypó prótou tinós arithmoú metreítai.)*

Em linguagem moderna, "todo número composto é divisível por algum número primo". O argumento de Euclides (de forma muito resumida) é: Se A é composto, algum número $B < A$ o divide. Se B é primo, terminamos. Senão, B é composto, e aplica-se a idéia novamente. Como uma sequência de números cada vez menores será gerada, em algum momento um número primo deverá ser encontrado, porque é impossível haver uma sequência infinita de inteiros,

O princípio da descida infinita é, essencialmente, o princípio da boa ordem, ligeiramente refraseado: "se algum processo iterativo gera, a partir de n, números naturais menores que n, então esse processo deve necessariamente parar".
As demonstrações dos Teoremas que seguem nesta seção ilustram o método. A primeira delas versa sobre triângulos retângulos, e necessita de um Lema de Euclides.
Antes da demonstração, definimos *tripla pitagórica*[32].

Definição 2.5 (tripla pitagórica)**.** *Sejam* $a, b, c \in \mathbb{Z}$*, com* $a, b, c > 0$*. Então* (a, b, c) *é uma* ***tripla pitagórica*** *se* $a^2 + b^2 = c^2$*. Quando* $\operatorname{mdc}(a, b, c) = 1$*, dizemos que é uma* ***tripla pitagórica primitiva****.* ◀

O Lema 2.2 determina que triplas pitagóricas sempre são compostas por dois números (na verdade, pode-se ler o Lema como um método[33] para obter triplas a partir de dois números co-primos m, n).

Lema 2.2 (fórmula de Euclides)**.** *Sejam* $a, b, c \in \mathbb{Z}$*, todos positivos. Então* (a, b, c) *são uma tripla pitagórica, ou seja,* $a^2 + b^2 = c^2$*, se e somente se existem* $m > n \in \mathbb{Z}$*,* $m, n > 0$*, um par e um ímpar, tais que*

$$\begin{aligned} a &= m^2 - n^2, \\ b &= 2mn, \\ c &= m^2 + n^2. \end{aligned}$$

O enunciado a seguir é de um Teorema que o próprio Fermat provou para ilustrar o método da descida infinita[34].

---

sendo o próximo sempre menor que o outro.

Euclid. **The Elements**. [*S. l.*]: Green Lion Press, 2002. Edição bilíngue Inglês/Grego.

[32] Muito provavelmente, o "Teorema de Pitágoras" não era nem teorema, e nem de Pitágoras. "Não era Teorema", porque não foi demonstrado inicialmente pelos pitagóricos. E "não era de Pitágoras", porque também não foi descoberto nem por Pitágoras e nem pelos outros pitagóricos (era conhecido bem antes deles).
A relação descrita no Teorema é descrita de diferentes maneiras em diferentes culturas, e em particular, os pitagóricos pareciam tratar o assunto de um ponto de vista aritmético, e não geométrico. Uma seção especificamente dedicada a isto é encontrada no livro de Tatiana Roque.

Roque, Tatiana. **História da Matemática: uma visão crítica, desfazendo mitos e lendas**. [*S. l.*]: Zahar, 2012.

[33] Este é o método discutido por Diofanto e Proclus. Pitágoras descrevia outro método, que gera algumas, mas não todas, as triplas primitivas: seja a ímpar, então a tripla é $\left(a^2, ((a-1)/2)^2, ((a+1)/2)^2\right)$.

[34] Fermat descreveu de forma superficial a demonstração, mas ela pode ser reconstruída a partir dali.

Teorema 2.6 (Fermat)**.** *Um triângulo retângulo com lados racionais não pode ter dois lados cada um com comprimento igual a um quadrado ou duas vezes um quadrado.*

Demonstração. Suponha que um triângulo como este exista. Podemos presumir que os lados são inteiros, multiplicando todos eles por algum quadrado (se o triângulo original for como no enunciado, o novo continuará sendo).
Se um primo p divide dois dos números, então deve dividir os três. Cancelamos os fatores em comum, presumimos que os lados são coprimos. Isso não mudaria o fato do triângulo ter dois lados quadrados ou dobro de quadrado: se p^2 está na fatoração de um dos lados, estará nas dos outros. Assim, cancelamos. Não chegaremos a cancelar todos os primos, porque chegaríamos a um triângulo $(1, 1, 1)$, que não seria retângulo. E ao cancelar p^2 de um lado quadrado, temos, se n é quadrado,

$$\begin{aligned} n &= a^2 p^2 \\ \frac{n}{p^2} &= a^2 \end{aligned}$$

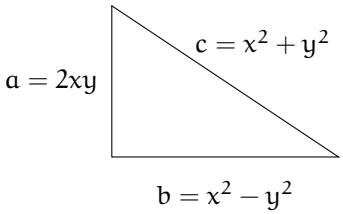
E se n é dobro de quadrado,

$$\begin{aligned} n &= 2a^2 p^2 \\ \frac{n}{p^2} &= 2a^2 \end{aligned}$$

E se $p = 2$, somente transformaremos dobro de quadrado em quadrado, mantendo a característica pedida no enunciado.
Pela fórmula de Euclides, existem dois inteiros coprimos positivos, um par e um ímpar, tais que

$$\begin{aligned} a &= x^2 - y^2, \\ b &= 2xy, \\ c &= x^2 + y^2. \end{aligned}$$

A tripla pitagórica é primitiva, porque determinamos que $\mathrm{mdc}\,(a, b, c) = 1$.
Então temos o seguinte triângulo, onde já indicamos a decomposição dos lados usando a fórmula de Euclides:

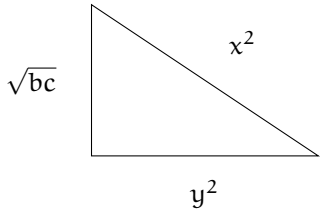


Mas b e c são ímpares, e não podem ser dobro de quadrado (e o enunciado determina que o triângulo tem dois lados que são ou quadrado ou dobro de quadrado). Temos portanto duas possibilidades:

i) b e c são quadrados;

ii) Somente um dentre b e c é quadrado.

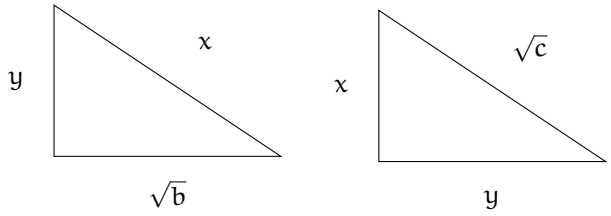
No caso (i) – se forem ambos quadrados – então encontramos um novo triângulo deste tipo:



Isso porque, como b e c são quadrados, podemos extrair sua raiz para construir um cateto, e a partir daí temos

$$\begin{aligned}\left(\sqrt{bc}\right)^2 + (y^2)^2 &= bc + y^4 && \text{(quadrados dos catetos)}\\ &= x^4 - y^4 + y^4 &&\\ &= x^4 &&\\ &= (x^2)^2. && \text{(quadrado da hipotenusa)}\end{aligned}$$

E no caso (ii) – se somente um deles for quadrado – e $a = 2xy$ for quadrado ou dobro de quadrado... Então um dentre x e y é quadrado ou dobro de quadrado, e um dos dois triângulos a seguir seria do mesmo tipo.



Nestes dois casos,

$$\begin{aligned}y^2 + (\sqrt{b})^2 &= y^2 + x^2 - y^2 && \text{(quadrados dos catetos)}\\ &= x^2 && \text{(quadrado da hipotenusa)}\end{aligned}$$

e, trivialmente,

$$x^2 + y^2 = c.$$

Em todos os casos, a hipotenusa é menor:

$$\begin{aligned} x^2 < c &= x^2 + x^2 \\ a < c &= x^2 + y^2 \\ \sqrt{c} < c & \end{aligned}$$

Como a medida da hipotenusa é um número inteiro, pelo princípio da descida infinita tal tipo de triângulo não pode existir. □

O Teorema 2.6, que acabamos de demonstrar, tem como consequência a inexistência de solução para a equação $x^4 + y^4 = z^4$ (que é uma instância do último Teorema de Fermat).
O próximo Teorema é mais simples, apresentado usualmente como forma de familiarizar estudantes com demonstrações.

Teorema 2.7. *$\sqrt{2}$ é irracional.*

Demonstração. (pelo método da descida infinita) Suponha que $\sqrt{2} \in \mathbb{Q}$. Então $\sqrt{2} = m/n$, sendo m/n uma fração reduzida: m e n são os menores números naturais tais que $m/n = \sqrt{2}$.

$$\begin{aligned} \sqrt{2} &= \frac{m}{n} \\ 2 &= \frac{m^2}{n^2} \\ 2n^2 &= m^2 \end{aligned}$$

O lado esquerdo é um quadrado par – e portanto o lado direito também é. Como m^2 só pode ser par se m for par, então podemos denotar $m = 2M$, e

$$\begin{aligned} 2n^2 &= (2M)^2 \\ 2n^2 &= 4M^2 \\ n^2 &= 2M^2 \end{aligned}$$

Agora, o lado direito é par, o que significa que o esquerdo também deve ser, e $n = 2N$: como $n = 2N$ e $M = 2M$,

$$\begin{aligned} \sqrt{2} &= \frac{m}{n} \\ &= \frac{2M}{2N} \\ &= \frac{M}{N}. \end{aligned}$$

Isso contradiz o que determinamos inicialmente – que m/n seria uma fração reduzida. O argumento usado nesta demonstração é que para cada m, n,

podemos gerar M e N, tais que $M < m$ e $n < N$, gerando uma quantidade infinita de números naturais cada vez menores.
Pelo princípio da descida infinita, essa sequência infinita não pode ser gerada, e a hipótese de $\sqrt{2}$ ser racional deve ser rejeitada.
Ou, da mesma forma, pelo princípio da boa ordem, o conjunto de números gerados neste processo é subconjunto de $\mathbb{N}$, e deve ter um menor elemento. Como o processo gera números cada vez menores, e não para, a hipótese deve ser rejeitada. □

Teorema 2.8. *Seja* $X = (x_1, x_2, \ldots, x_{2n+1})$ *uma sequencia com a seguinte propriedade: se* qualquer x_i *for removido, então a sequência resultante pode ser separada em duas sequências distintas* A *e* B*, cada um de tamanho* n*, tais que a soma de* A *e de* B *são iguais.*
Então $x_1 = x_2 = \cdots = x_{2n+1}$.

Por exemplo, em $(1, 2, 3, 3, 3)$ os elementos não são iguais. Se retirarmos 2, a sequência resultante é $(1, 2, 3, 3)$, que não pode ser particionada em duas sequências de mesma soma: quando a separarmos, teremos dois elementos em A e dois em B, e como são três ímpares e um par, as somas de A e B terão paridades diferentes, portanto serão diferentes:

A	B
$1 + 2 = 3$	$3 + 3 = 6$,
$1 + 3 = 4$	$2 + 3 = 5$.

Já a sequência $(2, 2, 2, 2, 2)$ tem todos os elementos iguais, e se removermos, por exemplo, o primeiro elemento, o resultado é $(2, 2, 2, 2)$, que pode ser dividida em duas subsequências de mesma soma, $(2, 2)$ e $(2, 2)$, ambas com soma 4 – e não há ourta forma de separar a sequência em duas.

Demonstração. Presuma, sem perda de generalidade, que os índices estão de acordo com a ordem dos números: $x_1 \leq x_2 \leq \cdots \leq x_{2n+1}$.
Suponha que haja na sequência pelo menos um elemento diferente de x_1.
Se removermos x_1 de todos os elementos, teremos

$$(0, x_2 - x_1, \ldots, x_{2n-1} - x_1),$$

e esta sequência ainda teria a mesma propriedade, porque removemos nx_1 tanto da soma de A como da de B.
Assim, trabalhamos com esta nova sequência onde $x_1 = 0$.
Agora, a soma de uma subsequencia de tamanho $2n$ será sempre par, porque de outra forma teríamos como obter A e B com paridades diferentes, e portanto somas diferentes.

Por consequência, quaisquer dois números x_i, x_j devem ter a mesma paridade, porque se não for o caso podemos trocar elementos entre os conjuntos A e B obtendo somas com paridades diferentes.
Mas como $x_1 = 0$ é par, então todos os x_i são pares. Se dividirmos todos os elementos por 2, a sequência manterá a propriedade.
Retomamos o processo, e a sequencia será dividida por 2 repetidamente.
Isso significa que os números serão divisíveis por 2, 2^2, 2^4, e por 2^k para qualquer k natural, gerando números pares cada vez menores. O único número divisível por 2^k para qualquer k (e que sempre geraria o zero, e não um natural menor) é o próprio zero, mas como havia algum elemento diferente de x_1, os x_i não poderão jamais ser todos iguais a zero.
Assim, todos os elementos são iguais a x_i. □

É comum expor explicitamente quando se pretende usar o método da indução, iniciando a demonstração dizendo que ela se dará "por indução na variável i", ou afirmação semelhante. Isso já não é tão comum quando se usa o princípio da descida infinita.

2.4 Inteiros e Racionais

Construiremos agora os números inteiros[35]. Podemos tentar fazê-lo de maneira muito simples: um inteiro é a diferença entre dois naturais. Temos $-2 = 0 - 2$ e $-5 = 10 - 15$, por exemplo. No entanto, isto não é aceitável, porque não definimos a operação de subtração para naturais (e se o tivéssemos feito, ela não seria fechada em $\mathbb{N}$).
Tentamos então construir inteiros como pares de naturais, e dois inteiros (a, b) e (p, q) são iguais se existe um número k tal que $b + k = a$ e $q + k = p$.
Permanece, entretanto, um problema: não podemos dizer que um inteiro é *um par ordenado de naturais* porque relacionamos mais de um par de naturais com o mesmo inteiro: tanto $(2, 3)$ como $(10, 11)$ seriam o mesmo inteiro, que usualmente denotamos por -1 (na verdade, desta forma obtivemos infinitos pares de naturais para cada inteiro).
Abraçamos a idéia do inteiro como vários pares ordenados, então. Para descrever quais pares ordenados de naturais definem o mesmo inteiro, usamos uma relação de quivalência.

Definição 2.6 (partição)**.** *Seja X um conjunto. Os conjuntos* $X_1, X_2, \ldots, X_k$ *são uma* ***partição*** *de X se*

i) todo X_i *é subconjunto de X;*

[35] Algumas vezes chamados de "inteiros racionais", para distinguí-los de inteiros de outros tipos. Por exemplo, um "inteiro Gaussiano" é um número complexo $a + bi$ onde $a, b \in \mathbb{Z}$; um "inteiro de Eisenstein" é um número complexo $a + b\omega$, onde $a, b \in \mathbb{Z}$, e ω é $(-1 + i\sqrt{3})/2$; há também outros tipos de número chamados de "inteiros" (inteiros ciclotômicos e inteiros Hamiltonianos são dois deles).

ii) *quando* $i \neq j$, $X_i \cap X_j = \emptyset$;

iii) *a união de todos os* X_i *é igual a* X. ◀

Exemplo 2.10. *Seja* P *o conjuntos dos naturais pares, e* I *o conjunto dos ímpares. Os conjuntos* P *e* I *formam uma partição de* $\mathbb{N}$*, porque*

i) $P \subset \mathbb{N}$, $I \subset \mathbb{N}$;

ii) $P \cap I = \emptyset$ *(não existe número que seja par e também ímpar);*

iii) $P \cup I = \mathbb{N}$.

O mesmo vale trivialmente para "primos e não primos", "quadrados perfeitos e não-quadrados", e também para partições em mais de dois subconjuntos, como no exemplo a seguir. ◀

Exemplo 2.11. *Podemos particionar* $\mathbb{N}$ *de forma que os números com* k *primos distintos em sua fatoração fiquem na* k*-ésima partição (admitindo* 0 *e* 1 *como suas próprias fatorações):*

i) *Na partição* P_1 *temos* 0, 1*, os primos e potências de primo:*

$$P_1 = \{0, 1, 2, 2^2, 2^3, 2^4, \ldots, 3, 3^2, 3^2, 3^4, \ldots, 5, 5^2, 5^3, 5^4, \ldots\}$$

ii) *Na partição* P_2 *temos* $6, 10, 12, 15$*, e os números com dois primos na fatoração:*

$$6 = (2)(3), 10 = (2)(5), 12 = (2^2)(3), 15 = (3)(5), \ldots$$

iii, ...) *E assim sucessivamente em outras partições* P_n.

Esta separação de $\mathbb{N}$ *em conjuntos é uma partição (facilmente verificável). Aqui,* $\mathbb{N}$ *é particionado em infinitos subconjuntos.* ◀

Definição 2.7 (relação de equivalência)**.** *Uma relação* R *em um conjunto* X *é* ***de equivalência*** *se, para todos* $x, y, z \in X$*,*

i) xRx *(*R *é reflexiva);*

ii) xRy *implica em* yRx *(*R *é simétrica);*

iii) xRy *e* yRz *implica em* xRz *(*R *é transitiva).* ◀

Exemplo 2.12. *Em* $\mathbb{N}$*, seja* $\sim$ *a relação definida tal que* $a \sim b$ *se e somente se, ao serem divididos por* 3*, tanto* a *como* b *deixam o mesmo resto. Assim,*

- $5 \sim 17$*, porque o resto de* 5 *por* 3 *é um, assim como o de* 17 *por 3;*
- $2 \sim 35$*, porque o resto de* 2 *por* 3 *é* 2*, assim como o de* 35 *por* 3.

A relação $\sim$, aqui definida, é de equivalência: para todos $m, n, o \in \mathbb{N}$,

i) $m \sim m$ *(é reflexiva);*

ii) se $m \sim n$*, então* $n \sim m$ *(é simétrica);*

iii) e se $m \sim n$*,* $n \sim o$*, então* $m \sim o$ *(é transitiva).*

Mais adiante este tipo de relação será tratada mais extensivamente. ◀

Exemplo 2.13. *Dois triângulos são* ***similares*** *se as proporções de seus lados são iguais – ou seja, se os comprimentos dos lados dos triângulos,* listados em ordem crescente *são* a, b, c *para o primeiro e* x, y, z *para o segundo, então os dois triângulos são similares se*

$$a/b = x/y$$
$$b/c = y/z$$
$$a/c = x/y$$

O conceito de simiaridade captura o que informalmente chamamos de "forma", abstraindo (ignorando) o tamanho dos triângulos.
Quando dois triângulos T_1 *e* T_2 *são similares, denotamos* $T_1 \sim T_2$*.*
Seja T *o conjunto de todos os triângulos. Então a relação de similaridade (a relação* $\sim$ *definida no parágrafo anterior) é de equivalência.*
Para cada três triângulos $A, B, C \in T$*,*

i) $A \sim A$*;*

ii) Se $A \sim B$*, então* $B \sim A$*;*

iii) Se $A \sim B$ *e* $B \sim C$*, então* $A \sim C$*,*

sendo os três itens trivialmente verificáveis. ◀

Teorema 2.9. *Seja* $\sim$ *uma relação de equivalência em um conjunto* X*, Então* $\sim$ define uma partição em X*, ou seja: se* $x \not\sim y$*, então* x *e* y *estão em partições diferentes; se* $x \sim y$*, estão na mesma partição. Todo elemento está em alguma partição, e as interseções entre partições são vazias.*

Exemplo 2.14. *A relação de similaridade entre triangulos, definida no Exemplo 2.13, é de equivalência, portanto define uma partição no conjunto* T *de todos os triangulos:*

i) toda partição é subconjunto de T*;*

ii) nenhum triângulo pode estar em duas classes diferentes de equivalência;

iii) a união de todas as classes de equivalência é T*.* ◀

Podemos agora voltar ao trabalho da definição dos inteiros.

Definição 2.8. *A relação* $\sim_+$ *entre números naturais é tal que* $(a, b) \sim_+ (p, q)$ *se e somente se* $a + q = p + b$. ◀

Teorema 2.10. $\sim_+$ *é relação de equivalência.*

Definição 2.9 (números inteiros)**.** *Sendo uma relação de equivalência,* $\sim_+$ *define uma partição em* $\mathbb{N} \times \mathbb{N}$*. Cada classe de equivalência nesta partição é um* ***número inteiro****.* ◀

Denotamos o conjunto dos números inteiros por $\mathbb{Z}$:

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N}) / \sim_+$$

Isto significa[36] que $\mathbb{Z}$ é igual a $\mathbb{N} \times \mathbb{N}$, mas com a relação de igualdade dada por $\sim_+$.
Temos agora números inteiros. Nos faltam as operações de soma e multiplicação, que não apresentam dificuldade:

$$(a, b) \oplus (p, q) = (a + p, b + q)$$
$$(a, b) \otimes (p, q) = (ap + bq, aq + bp)$$

Nesta definição, para evitar ambiguidade, usamos os símbolos $\oplus$ e $\otimes$ para operações com inteiros e $+$ para operações com naturais.
Os racionais são construídos de maneira semelhante, partindo de pares de inteiros. O Exercício 7 pede a definição da relação de equivalência $\sim_\times$ tal que os racionais possam ser construídos como $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}) / \sim_\times$.

2.4.1 Definições e Modelos

Há um problema que pode facilmente passar despercebido quando apresentamos a construção de um modelo para inteiros e racionais a partir dos naturais. Definimos inteiros como conjuntos, tendo como ponto de partida ao conjunto vazio. Mas os inteiros são pares ordenados. O natural dois é $\{0, 1\} = \{\emptyset, \{\emptyset\}\}$, e o inteiro dois é uma classe de equivalência inteira, $\{(2, 0), (3, 1), (4, 2), \ldots\}$. Como podemos considerá-los "iguais", se são entidades evidentemente diferentes? Não apenas são diferentes: um é finito e o outro não!
Diferenciamos a *definição* da *construção*. O que define os naturais são suas *propriedades*. As propriedades dos naturais são a de um semianel comutativo, que é o que precisamos para contar objetos e realizar operações aritméticas básicas com as quantidades que contamos. A partir do conjunto vazio, mostramos *uma* construção que tem as propriedades dos naturais. Se

[36] Dizemos que A/R é conjunto das partições de A, definido por R, e tem o nome de "conjunto quociente de A por R".

tomarmos os inteiros positivos apenas, teremos classes de equivalência que se comportam exatamente como os naturais – e portanto teremos uma outra construção dos naturais, *que depende da primeira*, porque afinal de contas, os pares ordenados contém os naturais-como-conjuntos de von Neumann.

2.5 Anéis e Corpos

Demonstramos a seguir um teorema simples a respeito de inteiros, e mais adiante esta demonstração nos servirá de motivação para definir uma generalização de $\mathbb{Z}$, chamada *anel*.

Teorema 2.11. *Em $\mathbb{Z}$, o inverso aditivo de qualquer elemento é único, ou seja, se $a + b = 0$ e $a + c = 0$ então $b = c$.*

Demonstração. Sejam $a, b, c \in R$, onde tanto b como c são inversos de a: $a + b = 0$ e $a + c = 0$. Então

$$\begin{aligned}
b &= b + 0 && (0 \text{ é neutro aditivo}) \\
&= b + (a + c) && (\text{premissa: } a + c = 0) \\
&= (b + a) + c && (\text{associatividade da soma}) \\
&= 0 + c && (\text{premissa: } b + a = 0) \\
&= c + 0 && (\text{comutatividade da soma}) \\
&= c, && (0 \text{ é neutro aditivo})
\end{aligned}$$

e quaisquer dois inversos aditivos para a serão iguais. Logo, os inversos aditivos em $\mathbb{Z}$ são únicos. □

Listamos as propriedades que usamos na demonstração:

- associatividade da soma;
- comutatividade da soma;
- existência de neutro aditivo (zero).

Isto significa que a demonstração deve valer sem mudanças para racionais, matrizes quadradas, polinômios, funções reais e outras estruturas que tenham as propriedades acima[37].
Uma *estrutura algébrica* é um conjunto adicionado de operações sobre seus elementos. Definimos estruturas algébricas para generalizar estruturas que encontramos na Matemática, abstraindo aquilo que elas tem em comum.

[37] Na verdade, nossa demonstração tratou de uma única operação, mas continuaremos trabalhando com estruturas com duas operações, para simplificar a exposição. No Capítulo 7 definiremos *grupo*, estrutura algébrica com somente uma operação onde a demonstração acima também vale.

Uma estrutura algébrica que tem as propriedades usadas na demonstração acima – e outras que nos interessam para tratar de inteiros – é o *anel*.

Definição 2.10 (anel)**.** *Um **anel** é um conjunto*[38] R *com duas operações* $\otimes$ *e* $\oplus$*, que denominamos "produto" e "soma", de forma que*

- *as duas operações são associativas;*
- *a operação de soma é comutativa;*
- *a multiplicação distribui sobre a soma;*
- *todo elemento tem um inverso para soma;*
- *existe um elemento neutro para soma.*

Se o anel tem elemento neutro para multiplicação, dizemos que é um anel com identidade[39]*.* ◀

Usamos a notação $\otimes$ e $\oplus$ na definição apenas para deixar claro que não é necessário que sejam a multiplicação e soma usuais.
Os inteiros, racionais e reais são claramente um anel. Além de conjuntos numéricos, há outros anéis relevantes:

- **Polinômios em uma variável**, com as operações usuais de soma e produto: o conjunto de todos os polinômios forma um anel. Por exemplo, denotamos por $\mathbb{R}[x]$ o conjunto de todos os polinômios na variável x (e nesta situação, os polinômios não é dada ateção ao "valor do polinômio para cada valor de x"; interessam apenas as *formas* dos polinômios, e como eles se comportam quando somados e multiplicados. A soma e a multiplicação de polinômios é comutativa e associativa; vale a distributividade; todo polinômio tem um inverso aditivo; e o polinômio 0 (zero) é o neutro aditivo
- **Funções de** $\mathbb{R}$ **em** $\mathbb{R}$: com as operações usuais de soma e multiplicação de funções, o conjunto de *todas* as funções $f : \mathbb{R} \to \mathbb{R}$ é um anel. Vários subconjuntos deste também são anéis. Por exemplo, o conjunto das funções reais contínuas.
- **Matrizes quadradas de ordem** n**:** também mantendo as operações usuais, fixado um n, o conjunto de todas as matrizes quadradas de ordem n é um anel não comutativo, com identidade.

Definição 2.11 (unidade)**.** *Uma **unidade** em um anel é um elemento com inverso multiplicativo. Ou seja,* a *é unidade se existe* b *tal que* $ab = 1$*, onde* 1 *é a identidade multiplicativa.* ◀

[38] A notação **não** é $\mathbb{R}$, mas sim R (remetendo à palavra "Ring").
[39] É mais comum o nome "anel com unidade", mas o termo "unidade" também é usado para elementos com inverso multiplicativo.

As unidades em $\mathbb{Z}$ são $+1$ e -1. No anel de matrizes quadradas com elementos em $\mathbb{R}$, as unidades são as matrizes invertíveis (e há infinitas unidades, portanto). No anel de polinômios $\mathbb{R}[x]$, são os polinômios constantes não nulos (também há infinitos deles).
A demonstração do Teorema 2.11 pode ser reescrita usando "um anel R" ao invés de "$\mathbb{Z}$", e vale portanto para qualquer anel.
Agora demonstramos outro teorema, desta vez sobre anéis.

Teorema 2.12. *Sejam R um anel e $0 \neq a \in R$. Suponha que haja um único $b \in R$ tal que $aba = a$. Então $ab = ba = 1$, ou seja, a é unidade (tem inverso multiplicativo igual a b).*

Se olharmos apenas para o anel dos inteiros, o Teorema não parece interessante, já que em $\mathbb{Z}$ somente o um tem inverso multiplicativo. Mas há outros anéis, portanto seguimos com a demonstração.

Demonstração. Suponha que $ax = 0$ para algum $x \in R$. Então

$$\begin{aligned} a(b+x)a &= (ab+ax)a && \text{(distributividade)} \\ &= aba + axa && \text{(distributividade)} \\ &= aba && \text{(ax=0)} \\ &= a && \text{(premissa: } aba = a\text{)} \end{aligned}$$

Ou seja, $a(b+x)a = a$. Como dissemos que b é o único tal que $aba = a$, então $b + x = b$, e $x = 0$.
Acima presumimos que $ax = 0$ e chegamos em $x = 0$ – ou seja, *sempre que $ax = 0$, teremos $x = 0$.*
Agora, reescrevemos ax com $x = (ba - 1)$:

$$\begin{aligned} a(ba-1) &= aba - a \\ &= a - a \\ &= 0 \end{aligned}$$

Como $a(ba - 1) = 0$, é necessário que $ba - 1 = 0$ – ou seja, $ba = 1$.
O argumento pode ser repetido, mostrando que $xa = 0$ implica em $x = 0$, e concluindo que $ab = 1$.
Demonstramos que $ab = ba = 1$, e consequentemente que a tem inverso multiplicativo b. □

Listamos as propriedades que usamos na demonstração:

- distributividade da multiplicação sobre a soma;

- associatividade da multiplicação (poderíamos ter expandido a primeira linha multiplicando os dois fatores da direita, mas fizemos com os dois da esquerda – o resultado é o mesmo);
- existência de neutro aditivo (zero);
- existência de neutro multiplicativo (um);
- $0x = x0 = 0$ para todo $x \in R$ (ou seja, o neutro aditivo aniquila R).

Não usamos comutatividade em nenhum momento. Isto significa que a demonstração deve valer para anéis não comutativos, como os anéis de matrizes quadradas!

Definição 2.12 (corpo)**.** *Um anel comutativo onde todo elemento diferente de zero tem inverso multiplicativo é um* ***corpo****.* ◀

Exemplo 2.15. *$\mathbb{Q}$, $\mathbb{R}$, e $\mathbb{C}$ são três corpos: são todos anéis comutativos, e em todos eles qualquer elemento diferente de zero tem inverso multiplicativo.* ◀

Exemplo 2.16. *O conjunto $\{0, 1\}$ com a operação de multiplicação usual, e com a soma definida como*

$$a \oplus b = \begin{cases} 0 & \text{se } a + b \text{ é par} \\ 1 & \text{se } a + b \text{ é ímpar} \end{cases}$$

é um corpo. ◀

Exemplo 2.17. *Embora $\mathbb{Z}$ seja um anel,* não é um corpo*, porque somente 1 tem inverso multiplicativo.* ◀

Exemplo 2.18. *O anel de matrizes quadradas de ordem n* não é um corpo*, porque nem toda matriz quadrada tem inversa, e também porque a multiplicação não é comutativa.* ◀

Exemplo 2.19. *(Subanel do anel dado no Exemplo 2.18) O anel de matrizes da forma*

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix},$$

onde $a, b \in \mathbb{Q}$ (ou $a, b \in \mathbb{R}$), com determinante não nulo é um corpo porque além de ser um anel, nele a multiplicação é comutativa; e todas as matrizes tem inversa (todas são unidade), exceto a matriz zero. ◀

Exemplo 2.20. *Uma função racional é uma função da forma*

$$f(x) = \frac{p(x)}{q(x)},$$

onde p *e* q *são polinômios, e* q *não é o polinômio nulo.*
O conjunto das funções racionais é um corpo. ◀

Exemplo 2.21. *Este exemplo é interessante porque, apesar de parecer artificial, por usar operações completamente diferentes das usuais, é usado na Geometria Tropical*[40]*.*
Seja

$$\mathbb{R}_{\text{trop}} = \{-\infty\} \cup \mathbb{R}.$$

E defina as operações

$$a \oplus b = \max(a, b),$$
$$a \otimes b = a + b.$$

Com estas operações,

- *O neutro* ***multiplicativo*** *é o zero (e não o um);*
- *O neutro* ***aditivo*** *é* $-\infty$*.*

O conjunto $\mathbb{R}_{\text{trop}}$ *com as duas operações definidas acima é um semi-corpo (seria um corpo se os elementos tivessem inversos para a operação* $\oplus$*, mas somente o próprio* $-\infty$ *tem), chamado de* ***corpo dos números tropicais*** *(apesar de não ser propriamente um corpo).* ◀

Exercícios

Ex. 1 — Usando os Axiomas de Dedekind-Peano, prove que nenhum número natural pode ser seu próprio sucessor.

Ex. 2 — Usando os Axiomas de Dedekind-Peano, prove que todo número diferente de zero é sucessor de algum outro.

Ex. 3 — Prove o Lema 2.2.

Ex. 4 — Prove que o Teorema 2.6 tem, de fato, como consequência, a inexistência de soluções para $x^4 + y^4 = z^4$.

Ex. 5 — A partir da relação $\leq$, defina $\geq$, $<$ e $>$ para naturais.

Ex. 6 — Prove o Teorema 2.3.

Ex. 7 — Construa os racionais usando pares de inteiros, como sugerido no final da seção 2.4: defina a relação de equivalência $\sim_\times$ e construa $\mathbb{Q} =$

[40] Não há nada em particular na referida geometria, ou na estrutura algébrica descrita, que tenha algo a ver com os trópicos. Geometria Tropical e Números Tropicais tem em seus nomes uma homenagem a Imre Simon, pesquisador brasileiro que trabalhou nesses tópicos[41].
[41] Trabalhou nos tópicos. E nos trópicos.

$\mathbb{Z}^2/\sim_\times$. Depois mostre as operações de soma e multiplicação para racionais, e mostre que as duas tem inversa em $\mathbb{Q}$.

Ex. 8 — Prove:

(a) $\forall n \geq 1,\ \ 3^n - 1$ é par.

(b) $\forall n \geq 1,\ \ n^3 + 2n$ é divisível por 3.

(c) $\forall n \geq 4,\ \ n! > 2^n$.

(d) $\forall n \geq x, \forall x \in \mathbb{R}$, se $x > -1$, então $(1+x)^n \geq 1 + nx$.

(e) $\forall n \geq 1,\ \ \sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$.

(f) $\forall n \geq 2,\ \ \prod_{i=2}^{n} \left(1 - \frac{1}{i^2}\right) = \frac{n+1}{2n}$.

Ex. 9 — Determine uma forma fechada para a soma dos n primeiros cubos ($1^3 + 2^4 + \cdots + n^3$), e demonstre sua validade usando indução.

Ex. 10 — Para cada caso, determine k e prove a afirmação, usando indução:

(a) Existe um número natural k tal que $n(n+1)(n+5)$ sempre é múltiplo de k, para todo n natural.

(b) Existe um número natural k tal que $9^n + 3$ sempre é múltiplo de k, para todo n natural.

Ex. 11 — (Fácil) Encontre uma bijeção entre triplas pitagóricas primitivas e os pontos racionais (isto é, pontos com coordenadas racionais) no círculo unitário. A partir disso, declare a cardinalidade do conjunto de triplas pitagóricas primitivas e do conjunto de todas as triplas pitagóricas (primitivas ou não).

Ex. 12 — Prove que exatamente um dos três números em uma tripla pitagórica é múltiplo de 5.

Ex. 13 — Se a, b são naturais, denotamos "b é múltiplo de a", ou "a divide b" por $a \mid b$, significando que existe algum k tal que $b = ka$. Prove que em $\mathbb{N}$, a relação $\mid$ é de ordem parcial não-estrita.

Ex. 14 — Prove que em qualquer anel, $-(-x) = x$.

Ex. 15 — Prove que em qualquer anel, o neutro aditivo é único.

Ex. 16 — Verifique se as estruturas a seguir são anéis (para cada uma, prove que é ou que não é). Quando não especificadas, as operações de soma e multiplicações são as usuais.

(a) $\mathbb{N}$.

(b) $\mathbb{C}$.

(c) Os inteiros pares.

(d) Os inteiros ímpares.

(e) Os reais não-negativos (está incluído o zero).

(f) O conjunto de todas as funções $f : \mathbb{R} \to \mathbb{R}$ tais que $f(x) = 0$ quando $x \in [3, 4]$.

(g) O conjunto de todas as funções reais integráveis em $[0, \infty]$.

(h) O conjunto de todas as funções reais ímpares (ou seja, $f(x) = -f(-x)$).

(i) O conjunto de todas as matrizes quadradas de ordem n, com determinante diferente de zero.

(j) O conjunto de todas as matrizes quadradas de ordem n, com determinante igual a ± 1.

(k) O conjunto de todas as matrizes quadradas com elementos inteiros.

(l) $\mathbb{R}$, mas com a operação de soma $a \oplus b = (a + b)/2$, onde $\oplus$ é a soma a ser usada na estrutura, e $+$ é a soma usual, que usamos apenas para definir $\oplus$.

(m) Tendo fixado um conjunto qualquer X, a estrutura que é composta do conjunto das partes de X, e das operações de diferença simétrica como adição e de interseção como multiplicação.

Ex. 17 — Matrizes quadradas de ordem n não formam um corpo, porque nem toda matriz tem inversa. E quanto ao conjunto das matrizes invertíveis?

Ex. 18 — Explique o significado de um polinômio "$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$" no (semi)corpo dos números tropicais, em termos de operações usuais[42] em $\mathbb{R}$?

[42] Não se preocupe com $-\infty$.

Capítulo 3

Bases

O sistema que usualmente empregamos para representar números é *posicional*[1] usando *base dez* – um número n é representado por dígitos concatenados, $n = d_k d_{k-1} \dots d_1 d_0$, com $0 \leq d_i < 10$, de forma que o valor de n é igual a

$$10^k d_k + 10^{k-1} d_{k-1} + \cdots + 10^1 d_1 + 10^0 d_0.$$

Por exemplo,

$$\begin{aligned} 2371 &= 10^3(2) + 10^2(3) + 10^1(7) + 10^0(1) \\ &= 2000 + 300 + 70 + 1 \end{aligned}$$

Há vários exemplos de sistema numérico não posicional. O mais evidente, talvez, seja o dos Romanos, onde[2] "IIII" significa $1 + 1 + 1 + 1 = 4$, e há a possibilidade de subtrair um número menor de um maior colocando o menor à esquerda ("IIX" é $10 - 2 = 8$).

Neste Capítulo provaremos que é possível usar qualquer natural maior que um como base, e não somente dez, resultando em diferentes sistemas para representação de números. Há exemplos de sistemas de numeração com bases diferentes usados no passado, como o de base 60, dos babilônios[3].

[1] O registro mais antigo de sistema posicional é dos babilônios.

Roque, Tatiana. **História da Matemática: uma visão crítica, desfazendo mitos e lendas**. [*S. l.*]: Zahar, 2012.

Capítulo 1: Matemáticas na Mesopotâmia e no antigo Egito.x

Boyer, Carl B. **A History of Mathematics**. [*S. l.*]: Wiley, 1991.

Capítulo 3: Mesopotamia.

[2] Não é verdade que os Romanos repetiam apenas 3 vezes o mesmo dígito. Era comum escrever IIII, XXXX, e assim por diante.

[3] O uso dominante de base dez é evidentemente derivado da anatomia humana, com dez dedos nas duas mãos, embora haja estudos mostrando que houve outros sistemas na História. Alguns povos nativos da América do Norte usavam base dois, três, cinco e vinte, por exemplo;

A representação de números em bases diferentes é relevante para Engenharias e Ciência da Computação, onde as bases 2 e 16 são extensamente usadas, mas também pode ser útil em demonstrações de teoremas[4].

3.1 Naturais

Mantendo o sistema posicional, podemos usar qualquer base maior ou igual a dois[5] para representar números naturais. Por exemplo, o número 10011 representa, na base dois, o natural dezenove:

$$\begin{aligned} & 2^4(1) + 2^3(0) + 2^2(0) + 2^1(1) + 2^0(1) \\ =& 16 + 0 + 0 + 2 + 1 \\ =& 19 \end{aligned}$$

Perguntamos agora se qualquer número natural pode ser representado em qualquer base. A resposta é sim[6], conforme o Teorema 3.1.

Teorema 3.1. *Seja* b *um número natural maior que um. Então todo número natural* n *pode ser descrito unicamente como*

$$n = a_0 b^0 + a_1 b^1 + \cdots + a_k b^k,$$

com $a_k \neq 0$ *e* $0 \leq a_i < b$. *Dizemos que esta é a* representação de n na base b.

os babilônios usavam base sessenta. Os maias, base vinte. Na França, o número oitenta é – ainda hoje – chamado de *quatre-vingt* (quatro-vinte), indicando talvez o uso em outros tempos de um sistema de base vinte (isso, no entanto, não explica outras irregularidades no francês, como os números entre setenta e setenta e nove – que em francês vão de "sessenta e dez" até "sessenta e dezenove" – "*soixante-dix*, . . . , *soixante-dix-neuf*". Ainda que não usando uma "base" (que implica em um sistema posicional), há registros de usos de "grupos" de várias quantidades – por exemplo, povos africanos usam grupos de três ou quatro.

Ore, Oystein. **Number Theory and Its History**. New York: Dover Publications, 1976.

Capítulo 1.
O Capítulo 1 do livro de Oystein Ore é uma boa fonte para a história dos sistemas de numeração.

[4] Por exemplo, a unicidade da representação em uma base pode ser usada para provar que o quociente e o resto da divisão de naturais são únicos. George Andrews faz isto no Capítulo 2 de seu livro.

Andrews, George. **Number Theory**. New York: Dover, 1994.

A representação em base 13 pode ser usada para provar que a recíproca do Teorema do valor intermediário não vale (como mencionado neste Capítulo).
A história da representação de números é contada, de forma resumida, por Oystein Ore.

Ore, Oystein. **Number Theory and Its History**. New York: Dover Publications, 1976.

Capítulo 1.

[5] Mas veja o Exercício 21.

[6] A resposta é a mesma para inteiros e racionais.

Demonstração. Primeiro demonstramos a *existência* de representação de n na base b; depois trataremos da *unicidade* dessa demonstração.
A existência de representação de n na base b é realizada por indução em n.
A base se dá com $n = 1$,

$$n = 1b^0 + 0b^1 + \cdots + 0b^k.$$

A hipótese de indução é

$$z = a_0b^0 + a_1b^1 + \cdots + a_kb^k, \qquad \text{para } z = 1, 2, \ldots, n-1.$$

Como presumimos que $b > 1$, então $b^0 < b^1 < b^2 < \cdots$, e todo natural maior que um está entre duas potências de b. Assim, seja $n > 1$ natural. Então existe um *único* q tal que

$$b^q \leq n < b^{q+1}.$$

Dividindo[7] n por b^q, obtemos quociente a_q e resto r:

$$n = a_qb^q + r, \quad 0 \leq r \leq b^q. \tag{3.1}$$

Observamos que
$a_q > 0$, porque $a_qb^q = n - r > 0$.
$a_q < b$, porque

$$\begin{aligned} a_qb^q &< n < b^{q+1} \\ a_qb^q &< b^{q+1} \\ a_q &< b. \end{aligned}$$

Quando $r = 0$, $n = 0b^0+0b_1+0b^2+\ldots+a_qb^q$, e a existencia da representação fica estabelecida para este caso.
Quando $r > 0$, sabemos que $r < n$ e portanto, pela hipótese de indução, r tem representação na base b:

$$r = d_0b^0 + d_1b_1 + d_2b^2 + \ldots + d_tb^t,$$

com $0 \leq d_i < b$ e $t \leq a$. Retomamos a Equação 3.1,

$$\begin{aligned} n &= r + a_qb^q, \\ &= \left(d_0b^0 + d_1b_1 + d_2b^2 + \ldots + d_tb^t\right) + a_qb^q, \end{aligned}$$

que é a representação de n na base b – e a existência fica estabalecida para

[7] Por ora presumimos que quociente e resto inteiros existem, e que o resto é menor que n. A demonstração rigorosa disso é dada no Capítulo 4

todos os casos.

Para a unicidade, presuma que n tem duas representações na base b,

$$n = e_0 + e_1 b + e_2 b^2 + \ldots + e_g b^g, + \ldots + e_{h-1} b^{h-1} + e_h b^h \quad (0 \leq e_i < b)$$
$$n = f_0 + f_1 b + f_2 b^2 + \ldots + f_g f^g, + \ldots + f_{h-1} b^{h-1} + f_h b^h \quad (0 \leq f_i < b).$$

onde admitimos que e_i possa ser zero para i entre $g+1$ e h (porque a representação usando os e_i é possivelmente mais "curta" do que aquela usando os f_j).

$$n = e_0 + e_1 b + e_2 b^2 + \ldots + e_g b^g, + \ldots + \left[0 b^{h-1} \quad + 0 b^h \right]$$
$$n = f_0 + f_1 b + f_2 b^2 + \ldots + f_g f^g, + \ldots + f_{h-1} b^{h-1} + f_h b^h,$$

Isto apenas permite que as representações tenham comprimentos diferentes (mas não necessariamente).

Subtraímos as duas representações, e devemos obter zero:

$$(e_0 - f_0) + (e_1 - f_1) b + (e_2 - f_2) b^2 + \ldots + (e_h - f_h) b^h = 0.$$

Denotamos $e_i - f_i$ por w_i, e temos

$$w_0 + w_1 b + w_2^2 + \ldots + w_h b^h = 0. \tag{3.2}$$

Considere o maior índice s tal que $e_s \neq f_s$ (ou seja, descarte a parte direita da soma onde os coeficientes são idênticos).

Se $s = 0$ (se descartamos todos os termos menos o primeiro), então $e_0 - f_0 = 0$, e portanto $e_0 = f_0$. As representações são idênticas.

Presumimos portanto $s > 0$. Como $0 \leq e_i < b$ e $0 \leq f_i < b$, temos

$$|w_i| = |e_i - f_i| \leq b - 1, \tag{3.3}$$

Como $s > 0$, existe pelo menos um i tal que $|w_i > 0$.

Reescrevemos a Equação 3.2 como

$$w_h b^h = -\left(w_0 + w_1 b + w_2^2 + \ldots + w_{h-1} b^{h-1} \right).$$

Agora verificamos que

$$\begin{aligned}
b^h &\leq \left|w_h b^h\right| \\
&= \left|w_0 + w_1 b + \cdots + w_{h-1} b^{h-1}\right| \\
&\leq |w_0| + |w_1 b| + \cdots + \left|w_{h-1} b^{h-1}\right| \\
&\leq (b-1) + (b-1)b + \cdots + (b-1)b^{h-1} && \text{(por 3.3)} \\
&= Z + Zb + \cdots + Zb^{h-1} && \text{(seja } Z = b-1\text{)} \\
&= \frac{Z(1-b^h)}{1-b} && \text{(soma de p.g.!)} \\
&= \frac{b-1}{1-b}(1-b^h) \\
&= b^h - 1,
\end{aligned}$$

o que é obviamente uma contradição. Concluímos que $e_i = f_i$ para todo i, e as representações são idênticas. □

3.2 Racionais positivos

A representação em diferentes bases também é possível para racionais positivos, bastando que usemos expoentes negativos. Na base dez, um número racional é representado por

$$\underbrace{10^k d_k + 10^{k-1} d_{k-1} + \cdots + 10^1 d_1 + 10^0 d_0}_{\text{parte inteira}} + \underbrace{10^{-1} f_1 + 10^{-2} f_2 + \cdots + 10^{-r} f_r}_{\text{parte fracionária}}.$$

Por exemplo,

$$\begin{aligned}
(2)10^2 + 0(10^1) + 3(10) \;+\; (5)10^{-1} + (1)10^{-2} &= 200 + 0 + 3 \;+\; (5)\frac{1}{10} + \frac{1}{100} \\
&= 203,51 \\
&= \frac{20351}{100}
\end{aligned}$$

Na base dois[8], o número $110,01$ representa

$$\begin{aligned}(1)2^2+(1)2^1+(0)2^0\ +\ (0)2^{-1}+(1)2^{-2} &= 4+2+0\ +\ (0)\frac{1}{2}+\frac{1}{4}\\ &= 6,25\\ &= \frac{625}{100}\\ &= \frac{25}{4}\end{aligned}$$

A representação de racionais em uma base usando o sistema posicional nem sempre é finita. Por exemplo, na base dez, $1/3$ é representado por $0,333\ldots$, havendo uma infinita sequência de dígitos 3; o racional $1/6$ é representado como $0,1666\ldots$, onde a sequência de dígitos 6 é inifita. Já em base 3, um terço é representado como $0,1$:

$$\begin{array}{rrl} 0 & \times 3^0 & = 0 \\ +1 & \times 3^{-1} & = 1/3 \end{array}$$

A caracterização desta situação requer a noção de primalidade, que será apresentada no Capítulo 5. Lá, o Teorema que determina quando a expansão em uma base é finita será apresentada (Teorema 5.2, na página 97).

É possível, no entanto, afirmar de imediato o Teorema 3.2. A demonstração é pedida no Exercício 30.

Teorema 3.2. *Se um número admite representação eventualmente periódica usando o sistema posicional em alguma base, ele é racional.*

Portanto, se a representação de um número em alguma base não é periódica, ele não é racional.

Neste contexto, "eventualmente periódica" pode ser inclusive "terminando com infinitos zeros", onde o zero é repetido com período um (por exemplo, $1/5 = 0.200000\ldots$).

3.3 A função base 13 de Conway

A função base 13 é uma surpreendente aplicação de mudança de base (de irracionais!), porque é um contraexemplo para a recíproca do Teorema do

[8] Em tempos passados, jogos de computador usavam representação de racionais em base dois com ponto fixo, porque o uso de ponto flutuante era caro demais (muito lento quando feito em software, e muito caro para adicionar ao hardware). Hoje todas as CPUs trabalham nativamente com representação em ponto flutuante, seguindo um padrão.

valor intermediário[9]. Ela foi inventada com este propósito[10] por Conway[11].

Teorema 3.3 (do valor intermediário)**.** *Se uma função* $f : \mathbb{R} \to \mathbb{R}$ *é contínua em um intervalo* $[a, b]$*, então dado um valor* d*, entre* $f(a)$ *e* $f(b)$*, sempre existe algum* c *tal que* $f(c) = d$*.*

A função base 13 *não* é contínua. Mas se $f(a) < f(b)$, então para todo x entre $f(a)$ e $f(b)$, sempre haverá um valor c tal que $f(c) = x$. Na definição da função fica claro que é usada a representação de *reais* em base 13. Embora não tenhamos abordado mudança de base para números reais, deve ficar evidente que a representação destes em diferentes bases se dá da mesma maneira que a representação de racionais, exceto que os irracionais tem expansão infinita[12].

Definição 3.1 (função base 13 de Conway)**.** *A* ***função base 13*** *de Conway,* $f : \mathbb{R} \to \mathbb{R}$ *é definida como segue. Para obter o valor de* $f(x)$*:*

- *Escreva o valor de* x *na base* 13 *(usando os signos* $A = 10$*,* $B = 11$*,* $C = 12$*).*
- *Se a partir de algum dígto na expansão de* x *na base* 13*, a sequência de dígitos for*

  $$A d_1 d_2 \ldots d_n C e_1 e_2 \ldots,$$

  sendo que todos os d_i *e* e_j *são dígitos em* $\{0, \ldots, 9\}$*, então*

  $$f(x) = d_1 d_2 \ldots d_n e_1 e_2 \ldots,$$

  ou seja, são removidos os dígitos A *e* C*.*
- *Se a expansão de* x *na base* 13 *for*

  $$B d_1 d_2 \ldots d_n C e_1 e_2 \ldots,$$

  sendo que todos os d_i *e* e_j *são dígitos em* $\{0, \ldots, 9\}$*, então*

  $$f(x) = -d_1 d_2 \ldots d_n e_1 e_2 \ldots,$$

- *Em outros casos,* $f(x) = 0$*.* ◀

[9] O Teorema do valor intermediário, do Cálculo.

[10] Uma revisão de trabalhos sobre a recíproca do Teorema do valor intermediário é dada por Grag Oman.

Oman, Greg. The Converse of the Intermediate Value Theorem: From Conway to Cantor to Cosets and Beyond. **Missouri Journal of Mathematical Sciences**, v. 26, n. 2, p. 134–150, 2014.

[11] John Conway (1937-2020), Britânico.

[12] Uma construção dos reais é dada no Capítulo 15.

As demonstrações de que esta função de fato é um contraexemplo para a recíproca do Teorema do valor intermediário são pedidas nos Exercícios 39 e 40.

Teorema 3.4. *A função f é descontínua em qualquer intervalo dado.*

Teorema 3.5. *Apesar de não satisfazer o antecedente do Teorema do valor intermediário, a função f satisfaz o consequente.*

Exercícios

Ex. 19 — Escreva o número 543 na base 4 e o número 111 na base 5.

Ex. 20 — Seja n representado, em base dez, por

$$d_k d_{k-1} \dots d_2 d_1 d_0.$$

Prove que n é divisível por 2^r se e somente se o número formado pelos dígitos $d_{r-1} \dots d_2 d_1 d_0$ também for divisível por 2^k. (Por exemplo, para $k = 2$: temos que um número é divisível por 4 se os dois últimos dígitos forem divisíveis por 4.)

Ex. 21 — Mostre como é possível representar qualquer número natural em base 1, desde que se abra mão do dígito zero (o que inclui abrir mão de representar a quantidade zero também).

Ex. 22 — Um número com mais de um dígito pode ter a mesma representação em duas bases? Mostre exemplo ou prove que não é possível.

Ex. 23 — Prove que, na base dez, o último dígito de um quadrado perfeito só pode ser $0, 1, 4, 5, 6$ ou 9.

Ex. 24 — Para quais valores de n, inteiro positivo, o número $1! + 2! + 3! + \dots + n!$ é quadrado perfeito?

Ex. 25 — Prove que o inverso de 7 não tem representação finita na base 60 (que é a base usada pelos babilônicos).

Ex. 26 — Que outros números, além de 7, não tem inverso com representação finita na base 60?

Ex. 27 — De maneira geral, que números não tem inverso com representação finita na base b?

Ex. 28 — Prove que qualquer número palíndromo na base dez, com quantidade par de dígitos, é divisível por onze.

Ex. 29 — Desenvolva a prova do Teorema 3.1.

Ex. 30 — Demonstre o Teorema 3.2.

Ex. 31 — Há um sistema posicional não padrão chamado de *ternário balanceado*. A base é 3, mas os coeficientes (dígitos) usados são $-1, 0, 1$. Pode-se denotar o dígito -1 por $\underline{1}$. Por exemplo:

$$\begin{aligned} \underline{1}1\underline{1}0 &= (-1)3^3 + (1)3^2 + (-1)3^1 + 0(3^0) \\ &= -27 + 9 - 3 + 0 \\ &= -21 \end{aligned}$$

A tabela a seguir dá outros exemplos.

base 10	ternário balanceado
$\vdots$	
-5	$\underline{1}11$
$\vdots$	
-1	$\underline{1}$
0	0
1	1
2	$1\underline{1}$
3	10
4	11
5	$1\underline{11}$
$\vdots$	

(a) Escreva os números $-3, -8, +8, +11$ em representação ternária balanceada.

(b) Prove que se a representação ternária balanceada de $-n$ é igual à de n, trocando-se apenas os sinais dos coeficientes (ou seja, trocando 1 por $\underline{1}$ e vice-versa).

(c) Prove que esta representação permite expressar todos os inteiros.

(d) Prove que a representação ternária balanceada de um número inteiro é única.

(e) É possível representar racionais em base ternária balanceada? Mostre como, ou prove que não é possível.

Ex. 32 — Quantos dígitos são necessários para representar o número $n \in \mathbb{N}$ na base k?

Ex. 33 — A representação de racionais em sistema posicional com vírgula é única em qualquer base? Se há exceções, quais são?

Ex. 34 — Que números são representáveis, usando o sistema posicional, por uma base racional (e não inteira) m/n, com $m, n \in \mathbb{Z}$? Por exemplo, se a base é $2/3$, números seriam da forma

$$a_0 + a_1\frac{2}{3} + a_2\left(\frac{2}{3}\right)^2 + a_3\left(\frac{2}{3}\right)^3 + \cdots$$

O conjunto é infinito, mas é igual a $\mathbb{R}$? Igual a $\mathbb{Q}$? Ou, pode-se pelo menos determinar algum conjunto de números que certamente é (ou não é) representável?

Ex. 35 — Usando dez dígitos, $0, 1, \ldots, 9$, e vinte e seis letras, $A, B, \ldots, Z$, é possível escrever números em base 36, usando um dos 36 símbolos em cada posição. Assim, os dígitos tem seus valores usuais, e as letras valem

A	B	C	$\cdots$	X	Y	Z
10	11	12	$\cdots$	33	34	35

Desta forma, a representação do número 157 em base 36, usando o esquema descrito, é 4D, porque

$$\begin{aligned}(4)36^1 + (\mathrm{D})36^0 &= (4)36^1 + (13)36^0\\ &= 144 + 13\\ &= 157.\end{aligned}$$

Agora, na base 36, o quadrado de

$$\underbrace{111111111111111111111111111111111}_{35\text{ uns}}$$

é o palíndromo

$$\begin{aligned}&1234567\,89ABCDE\,FGHIJKL\,MNOPQRS\,TUVWXY\,Z\\ &YXWVUT\,SRQPONM\,LKJIHGF\,EDCBA98\,7654321\end{aligned}$$

Isso pode ser generalizado para qualquer base? Se não for verdade, mostre contraexemplo. Se for verdade, formalize e demonstre.

Ex. 36 — Seja $111\ldots111$ a representação de um natural n na base k, sendo k maior que a quantidade de uns na representação de n. Qual é a representação de n^3 na mesma base? Demonstre.

Ex. 37 — Existe um sistema de representação de números chamado de *representação binária com ponto fixo*, que é uma variante da representação de racionais que abordamos neste capítulo. A representação usa zeros e uns; um número tem n dígitos antes do ponto decimal, e m dígitos depois

dele. O número

$$a_{n-1} \dots a_2 a_1 a_0 \, . \, a_{-1} a_{-2} \dots a_{m-1} a_{-m}$$

é igual (da mesma forma que na representação binária de inteiros) a

$$\sum_{-m \leq i \leq n-1} a_i 2^i$$

Por exemplo, com $n = 3$ e $m = 2$,

$$\begin{aligned} 101.011 &= 1(2^2) + 0(2^1) + 1(2^0) \quad + \quad 0(2^{-1}) + 1(2^{-2}) + 1(2^{-3}) \\ &= 4 + 0 + 1 \quad + \quad 0 + \frac{1}{4} + \frac{1}{8} \\ &= 5 + \frac{3}{8} \\ &= 5.375. \end{aligned}$$

a) Mostre que se m e n forem fixos, as operações de soma e multiplicação não são associativas.

b) Tome $m = 3$ e $n = 6$. Tente dar uma estimativa do erro, $|(ab)c - a(bc)|$, em função de a, b.

Ex. 38 — Há uma *Lei de Newcomb-Benford*, que afirma que os números em certos conjuntos de dados que surgem naturalmente apresentam a seguinte propriedade: a distribuição do **primeiro** dígito é dada pela *distribuição de*

Newcomb-Benford[13]

$$\Pr(d) = \log_{10}\left(1 + \frac{1}{d}\right),$$

[13]Em 1881 o astrônomo Newcomb[14]Simon Newcomb observou que os livros com tabelas de logaritmos tinham páginas iniciais muito mais desgastadas do que as finais, e que portanto os números iniciando com 1 eram mais frequentemente buscados – e portanto ocorriam mais frequentemente. Newcomb chegou a determinar as probabilidades para os primeiros e segundos dígitos de números, e terminou seu artigo mencionando que

> *É curioso observar que esta lei nos permitiria decidir se uma grande coleção de resultados numéricos independentes foi composta por números naturais ou logaritmos.*

No original,

> *It is curious to remark that this law would enable us to decide whether a large collection of independent numerical results were composed of natural numbers or logarithms.*

Newcomb, Simon. Note on the Frequency of Use of the Different Digits in Natural Numbers. **American Journal of Mathematics**, v. 4, n. 1, p. 39–40, 1881.

Este fenômeno ficou conhecido como "Lei de Benford" porque observações semelhantes foram feitas em 1938 por Benford[15], com números de diferentes origens.

Benford, Frank. The Law of Anomalous Numbers. **Proceedings of the American Philosophical Society**, v. 78, n. 4, p. 551–572, 1938.

O nome de Benford ficou mais fortemente associado ao tema (fala-se da "Lei de Benford"), embora Newcomb tenha feito sua observação muito tempo antes de Benford. Isso possivelmente se deu porque Benford mostrou não apenas uma observação teórica, mas sua publicação reuniu várias observações em diferentes contextos, trazendo portanto estudos empíricos, fortalecendo a idéia de que aquela parecia ser uma "lei universal", e principalmente, apontando para seu potencial de uso prático. Além disso, o Seculo XIX tinha meios de comunicação científica mais limitados, menos periódicos amplos, e não havia as muitas conferências do Século XX. Benford, ao divulgar o resultado, tinha tudo isso para potencializar a difusão, e consequentemente seu nome ficou associado ao achado. Talvez, em um sentido Bourdiesiano, pode-se dizer que a estrutura do campo e o capital científico diferiam muito nas duas épocas, e que Benford estava em um campo mais institucionalizado, que facilitava a conversão de publicações em capital simbólico. Sobre o "pragmatismo" e visão aplicada de Benford, faz sentido pensar, de um ponto de vista Foucaultiano, que o regime discursivo que determina autoridade científica ficou mais amplo e institucional, permitindo que concepções e objetos científicos com aplicação prática sejam rapidamente incorporados ao "discurso verdadeiro". Ainda sobre a diferença entre Matemática pura e aplicada, a exposição de Hardy[16] em "Apologia de um Matemático" é interessante: Hardy diz ver mais elegância e beleza na Matemática pura do que na aplicada, e também coloca a percepção de que a Matemática pura é menos suscetível a aplicações danosas à humanidade (como a guerra – Hardy era um pacifista).

Hardy, G. H. **A Mathematician's Apology**. [*S. l.*]: Cambridge University Press, 1940.

ou seja,

$$\begin{aligned}
\Pr(1) &\approx 0.301 \\
\Pr(2) &\approx 0.176 \\
\Pr(3) &\approx 0.125 \\
\Pr(4) &\approx 0.097 \\
&\vdots
\end{aligned}$$

Prove que esta propriedade, quando presente em um conjunto de números, é invariante por base (ou seja, se um conjunto de números apresenta esta propriedade, e todo o conjunto for reescrito em base diferente da base 10, a Lei de Benford continuará valendo, exceto que o logaritmo deverá ser tomado na nova base, e não na base dez)[17].

Ex. 39 — Prove o Teorema 3.4.

Ex. 40 — Prove o Teorema 3.5.

[17] Isto é relevante em detecção de fraudes. Um conjunto de dados respeitar a Lei de Benford *somente na base dez* é diferente de um conjunto de dados respeitar a Lei de Benford *em qualquer base*. Como exemplo, nas as eleições para o Senado Brasileiro em 1994 houve um caso(no estado da Bahia) em que a Lei de Benford não se verifica em diferentes bases, diferentemente do que ocorre com outras eleições para o mesmo cargo em estados diferentes.

Gueron, Eduardo; **Pellegrini**, Jerônimo. Application of Benford − Newcomb law with base change to electoral fraud detection. v. 607, 2022. Preprint disponível em `https://arxiv.org/abs/2207.05524v2`.

Uma análise das eleições brasileiras desde o início do uso da urna eletrônica mostra que as eleições passaram a respeitar Benford em todas as bases.

Gueron, Eduardo; **Pellegrini**, Jerônimo; **Aristimunha**, Bruno. Distribuição de Newcomb-Benford, Mudanças de Bases e Aplicações Eleitorais. *In:* 1. PROCEEDING Series of the Brazilian Society of Computational and Applied Mathematics. Bonito - MS: [*s. n.*], 2023. v. 10. Trabalho apresentado no XLII CNMAC.

Parte I

Capítulo 4

Divisibilidade

Neste Capítulo, após definir divisão, tratamos do conhecido conceito de "máximo denominador comum", e apontamos um caso onde ele é relevante fora do anel dos inteiros.
Nos enunciados deste Capítulo não incluímos a usual qualificação de elementos como inteiros ("$a, b \in \mathbb{Z}$"). Podemos presumir que *todos* os elementos são inteiros, a não ser que determinemos o contrário. Mais ainda, pode-se ler o Capítulo como se todos estes elementos fossem membros de um anel ordenado comutativo com unidade. Eventualmente damos exemplos usando o anel[1] $\mathbb{R}[x]$ sem abordar ordem. Na Seção 4.6 outras estruturas são descritas.

4.1 Divisão

A noção de divisibilidade é fundamental em Teoria dos Números.

Definição 4.1 (divisibilidade)**.** *Dizemos que* a ***divide*** b *(denotamos* $a \mid b$*) se existe* c *tal que* $ac = b$*. Quando* a *não divide* b*, denotamos* $a \nmid b$*.* ◀

Da definição concluímos que *zero divide zero* ($0 \mid 0$), porque existem infinitos c tal que $0c = 0$. No entanto, justamente por haver infinitas possibilidades para c, não definimos *a operação de divisão* de zero por zero. Isto pode ficar mais claro se não lermos "$a \mid b$" como "a divide b", mas como "a tem múltiplo b".
Como exemplo em $\mathbb{Z}$, $3 \mid 15$ porque $3(5) = 15$; já $4 \nmid 10$, porque não existe inteiro k tal que $4k = 10$.

[1] Um conjunto de polinômios em uma variável é um anel. Por exemplo $\mathbb{R}[x]$ é o conjunto de todos os polinômios em uma variável real.

Para um exemplo no anel $\mathbb{R}[x]$ (polinômios na variável x com coeficientes em $\mathbb{R}$), temos $(x-1) \mid (x^3 - x^2)$, porque

$$(x-1)x^2 = x^3 - x^2.$$

Em $\mathbb{Z}$, $4 \mid 20$, porque $4(5) = 20$.
O seguinte Teorema trata de alguns fatos básicos a respeito de divisibilidade, e é deixado como exercício.

Teorema 4.1. *Para todos* a, b, c*:*

(i) *Se* $a \mid b$ *então* $a \mid bc$.

(ii) *A relação* $\mid$ *é transitiva.*

(iii) *Se* $a \mid b$ *e* $b \mid a$*, então* $a = \pm b$.

(iv) *Se* $b \neq 0$ *e* $a \mid b$ *então* $|a| \leq |b|$.

(v) *Para todo* $m \neq 0$*, será verdade que* $a \mid b$ *se e somente se* $ma \mid mb$.

(vi) *Para todo* $a \neq 0$ *tal que* $a \mid (b+c)$*, será verdade que* $a \mid b$ *se e somente se* $a \mid c$

O Lema a seguir é simples, mas bastante útil.

Lema 4.1. *Se* $a \mid b$ *e* $a \mid c$*, então* $a \mid (xb + yc)$.

Demonstração. Pela definição de divisibilidade, se $a \mid b$ e $a \mid c$ então há m, n tais que $ma = b$ e $na = c$. Então

$$\begin{aligned} xb + yc &= x(ma) + y(na) \\ xb + yc &= a(xm + yn) \\ a &\mid (xb + yc) \end{aligned}$$

□

O Teorema a seguir trata da divisibilidade de somas e diferenças de potências, e será importante mais adiante.

Teorema 4.2. *Para todo* $n \in \mathbb{N}$ *e para todos* a, b, c*,*

(i) $(a-b) \mid (a^n - b^n)$

(ii) $(a+b) \mid a^{2^n+1} + b^{2^n+1}$

(iii) $(a+b) \mid a^{2n} - b^{2n}$

Demonstração. Demonstramos apenas (i); os outros dois itens são exercícios.

(i) Por indução em n: $(a-b) \mid (a^0 - b^0) = 0$, porque todos dividem o zero; A hipótese é $(a-b) \mid (a^n - b^n)$.

$$\begin{aligned} a^{n+1} - b^{n+1} &= aa^n - bb^n \\ &= aa^n - ba^n + ba^n - bb^n \\ &= (a-b)a^n + b(a^n - b^n) \\ &= X(a-b) + Y(a^n - b^n) \\ &= X(a-b) + Z(a-b) \qquad \text{(por hipótese, } (a-b) \mid (a^n - b^n)\text{)} \\ &= (X+Z)(a-b), \end{aligned}$$

e portanto $(a-b) \mid (a^{n+1} - b^{n+1})$. □

O Teorema da Divisão garante que sempre há como efetuar a divisão com resto de a por b, resultando em um quociente q e resto r.

Teorema 4.3 (da Divisão)**.** $\forall b \neq 0, a$*, existem* q, r *únicos tais que* $a = qb + r$*, com* $0 \leq r < |b|$.

Demonstração. Primeiro determinamos a <u>existência</u> de r e q. O resto, r, deve ser não-negativo e da forma $a - qb$; considere então todos os números da forma $a + kb$, com $k \in \mathbb{Z}$:

$$S = \{\ldots, a-3b, a-2b, a-b, a, a+b, a+2b, a+3b, \ldots\}. \tag{4.1}$$

Tome o subconjunto de S contendo somente os elementos não-negativos. Este conjunto é subconjunto de $\mathbb{N}$, onde todos os elementos sào da forma $a+qb$. Mas sendo subconjunto não-vazio de $\mathbb{N}$, pelo princípio da boa ordem, contém um menor elemento, a quem chamamos de r. A partir de r podemos imediatamente computar o quociente q.
Mostraremos agora que $r < |b|$: suponha que o r encontrado seja maior ou igual a $|b|$. Então

$$r' = r - |b|$$

também seria da mesma forma, e não é negativo (porque $r \geq |b|$). Logo, r não era o menor não-negativo do conjunto, como presumido inicialmente.
Falta demonstrar a <u>unicidade</u> de q e r. Presumiremos que também há q'' e r'' tais que $a = qb'' + r''$, e mostraremos que $r'' = r$, o que por sua vez implica que $q'' = q$.
Se há dois restos r, r'', então sem perda de generalidade, presumimos que $r < r''$, e portanto

$$0 < r'' - r < |b|.$$

Agora, temos duas expressões para a:

$$a = qb + r, \quad a = q''b + r''.$$

Estas nos dão fórmulas para r e r'':

$$r = a - qb, \quad r'' = a - q''b.$$

Calculamos $r'' - r$, e obtemos $(a - q''b) - (a - qb) = qb - q''b = b(q - q'')$, e portanto $b \mid (r'' - r)$. como sabemos que tanto r como r'' são não-negativos e estritamente menores que $|b|$, então

$$\begin{aligned} -|b| < r'' - r < |b| & \\ -|b| < Kb < |b|, & \qquad \text{(porque } b \mid (r'' - r)\text{)} \end{aligned}$$

mas o único múltiplo de b que poderia ser $r'' - r$ é zero (ou seja, o único $K \in \mathbb{Z}$ possível é zero). Logo, $r'' = r$ e $q'' = q$. □

Tendo provado que sempre é possível dividir dois inteiros (ou dois elementos de um anel comutativo), podemos definir a operação de divisão.

Definição 4.2 (divisão)**.** *Dizemos que a a* ***divisão*** *de a por $b \neq 0$ resulta em* ***quociente*** *q com* ***resto*** *r quando $a = qb + r$.* ◀

Exemplo 4.1. *A divisão de 13 por 5 resulta em quociente 2, com resto 3, porque $13 = 2(5) + 3$.* ◀

4.2 Máximo Divisor Comum

Definimos agora o máximo divisor comum entre dois ou mais elementos, e apresentamos o algoritmo de Euclides para calculá-lo. O MDC é o maior elemento que divide um conjunto de elementos – isto fica definido com mais clareza a seguir.

Definição 4.3 (máximo divisor comum)**.** *d é o* ***máximo divisor*** *comum de a e b se*

(i) *d não é negativo;*

(ii) *$d \mid a$, $d \mid b$;*

(iii) *se $k \mid a$ e $k \mid b$, então $k \mid d$.* ◀

Exemplo 4.2. *Em $\mathbb{Z}$, temos $\operatorname{mdc}(28, 12) = 4$, porque $4 \mid 28$, $4 \mid 12$, mas os únicos outros números que dividem 28 e 12 são 1 e 2 – e ambos dividem 4.* ◀

Teorema 4.4. *Se pelo menos um dentre a, b for diferente de zero, então $\operatorname{mdc}(a, b)$ é único.*

Demonstração. Suponha que existam dois números satisfazendo a definição de $\mathrm{mdc}(a,b)$, d_1 e d_2. Pela mesma definição, como $d_2 \mid a$ e $d_2 \mid b$, então $d_2 \mid d_1$. Mas semelhantemente, $d_1 \mid d_2$. Como os dois são positivos, $d_2 \mid d_1$ e $d_1 \mid d_2$ implica que $d_1 = d_2$. □

Note que o final da demonstração não é válido para qualquer anel: em $\mathbb{R}[x]$, considere os polinômios x e $2x$. Temos $x \mid 2x$, também $2x \mid x$, e $x \neq 2x$. Neste caso, não valerá a unicidade do MDC.
Nesta demonstração excluímos a possibilidade de $a = b = 0$. O Exercício 55 pede para elaborar o motivo dessa restrição.
O próximo resultado relevante a examinar é o Lema de Bézout[2][3]. Definimos, para isso, o conceito de *combinação linear inteira*[4].

Definição 4.4 (combinação linear inteira)**.** *Uma* ***combinação linear inteira*** *de dois elementos a e b é $xa + yb$, onde $x, y \in \mathbb{Z}$.* ◀

Lema 4.2 (de Bézout)**.** *Para todos $a, b \in \mathbb{Z}$, $\mathrm{mdc}(a,b)$ é combinação linear inteira de a e b – ou seja, existem $x, y \in \mathbb{Z}$ tais que $\mathrm{mdc}(a,b) = xa + yb$.*

[2] Étienne Bézout (1730-1783), Francês.
[3] Na verdade Bézout provou a afirmação para polinômios.

Bézout, Etienne. **Théorie Générale des Équations Algébriques**. [*S. l.*], 1779. Disponível em https://archive.org/details/thoriegnra00bz.

Quem demonstrou este lema para números inteiros foi Claude Gaspar Bachet, em 1612.

Bachet, Claude Gaspar (Sr de Meziriac). **Problèmes plaisans et deléctables, qui se font par les nombres**. [*S. l.*], 1612. Disponível em https://archive.org/details/bub_gb_Zy0PAAAAQAAJ.

Na página 129,

> *Sendo dados dois números primos entre eles, encontre um múltiplo de qual deles você deseja, que supere o outro pela unidade, ou algum múltiplo do outro.*

O original de Bachet é:

> *Deux nombres premiers entre eux estant donnez, trouver un multiple daquel d'iceux qu'on voudra, qui surpasse l'autre de l'unité, ou quelque multiple de l'autre.*

Isto equivale a resolver $a = by + 1$, ou $a - by = 1$, para a e b coprimos.
Em 1612 Bachet já listava "teoremas" e "demonstrações". O livro contém uma lista de teoremas, seguida de uma lista de problemas, que são expostos à maneira da época – por exemplo,

> **PROBLEMA I:** *Adivinhar o número que alguém tiver pensado.*

O original é:

> **PROBLEME I:** *Deviner le nombre que quelcun aura pensé.*

Aqui, por exemplo, Bachet propõe uma brincadeira simples, onde pede que alguém pense em um número e faça operações. A partir do resultado, pode-se determinar o número original. Na segunda edição do livro, Bachet demonstra o teorema.

[4] Em um espaço vetorial, a combinação linear $au + bv$ de vetores resulta em outro vetor w. Se permitirmos apenas combinações lineares inteiras, os vetores formarão um **reticulado**: Se $B = \{b_1, b_2, \ldots, b_n\}$ é uma base para $\mathbb{R}^n$, então $\mathcal{L} = \{a_1 b_1 + a_2 b_2 + \cdots + a_n b_n : b_i \in B, a, b \in \mathbb{Z}\}$ é um reticulado de dimensão n. Pode-se, claro, trocar $\mathbb{R}$ por outro corpo.

A demonstração do Lema de Bézout será acompanhada de comentários para auxiliar a compreensão de sua estrutura (estes não serão comuns no resto do texto, mas apenas neste momento inicial): partimos de a e b, e mostramos que existem x e y que atendem a definição de MDC: identificaremos um elemnto z no conjunto de todas as possíveis combinações lineares $xa + yb$, e mostraremos que (1) $z \geq 0$; (2) z divide tanto a como b; e (3) finalmente, mostraremos que (3) se existe k tal que $k \mid a$ e $k \mid b$, então $k \mid z$.

Demonstração. Seja $S = \{xa + yb \ : \ x, y \in \mathbb{Z}\}$. Seja z o menor elemento positivo de S. Então existem $x, y \in \mathbb{Z}$ tais que $z = xa + yb$.
Agora presuma que $z \nmid b$. Então a divisão de b por z deve ter resto diferente de zero, ou seja, $b = qz + r, \ \ 0 < r < z$. Logo,

Temos (1) $z > 0$

$$\begin{aligned} r &= b - qz \\ &= b - q(xa + yb) \\ &= b - qxa - qyb \\ &= (1 - qy)b - (qx)a \\ &\in S. \end{aligned}$$

Mas como $r \in S$, e $r < z$, temos uma contradição, porque havíamos tomado z como o *menor* elemento positivo de S. Desta forma negamos nossa suposição e concluímos que $z \mid b$. O argumento que fizemos para b pode ser repetido para a, obtendo $z \mid a$.

Provamos (2) $z \mid a$ e $z \mid b$

Agora temos um elemento (z) que divide tanto a como b, e que é não negativo. Falta mostrar que se $k \mid a$ e $k \mid b$, então $k \mid z$, o que segue imediatamente porque $z = xa + yb$. □

Provamos (3), $k \mid a$, $k \mid b$ $\Rightarrow k \mid z$

Exemplo 4.3. *O MDC de 24 e 36 é 12, que é combinação linear de 24 e 36:*

$$(-1)24 + (+1)36 = 12,$$

onde os coeficientes de Bézout são -1 e $+1$.
O MDC de 93 e 306 é 3, que é combinação linear de 93 e 306:

$$(-23)93 + (+7)306 = 3,$$

e os coeficientes de Bézout são -23 e $+7$. ◀

Corolário 4.1. $\mathrm{mdc}\,(a, b)$ *é o menor valor positivo dentre todas as combinações lineares inteiras de a e b:*

$$\mathrm{mdc}\,(a, b) = \min_{x,y \in \mathbb{Z}} \{xa + yb\} \cap \mathbb{N} \setminus \{0\}.$$

Corolário 4.2. *A equação $ax+by = c$ tem solução se e somente se* $\mathrm{mdc}\,(a, b) \mid c$.

Demonstração. Suponha que $ax + by = c$, e que $d = \mathrm{mdc}\,(a, b)$. Como $d \mid a$ e $d \mid b$, então $d \mid (ax + by) = c$.
Agora, se $\mathrm{mdc}\,(a, b) = d \mid c$, então $c = nd$. Mas pelo Corolário 4.1 deve haver w, z tais que $aw + bz = d$, e portanto $a(wn) + b(zn) = nd = c$. □

O Exercício 61 pede a demonstração do Teorema 4.5, que nos será útil adiante.

Teorema 4.5. *Para todos* a, b, m, $\mathrm{mdc}\,(ma, mb) = m\big(\mathrm{mdc}\,(a, b)\big)$.

Exemplo 4.4. *Sejam* $a = 10$, $b = 25$ *e* $m = 3$.

$$\mathrm{mdc}\,(a, b) = \mathrm{mdc}\,(10, 25) = 5,$$

portanto

$$\begin{aligned}\mathrm{mdc}\,(ma, mb) &= \mathrm{mdc}\,((3)10, (3)25)\\ &= \mathrm{mdc}\,(30, 75)\\ &= 15\\ &= (3)(5)\\ &= m(\mathrm{mdc}\,(ma, mb)).\end{aligned}$$ ◀

Teorema 4.6. *Se* $\mathrm{mdc}\,(b, c) = 1$ *e* $c \mid ab$ *então* $c \mid a$.

Demonstração. Do enunciado,

$$\begin{aligned}\mathrm{mdc}\,(b, c) &= 1\\ a\,\mathrm{mdc}\,(b, c) &= a\\ \mathrm{mdc}\,(ab, ac) &= a \qquad \text{(Teorema 4.5)}\end{aligned}$$

O enunciado determina que $c \mid ab$; temos também que $c \mid ac$, pela definição de divisibilidade; logo, c é divisor de ab e ac. Mas $\mathrm{mdc}\,(ab, ac)$ é a, e pela definição de MDC, todos os outros divisores de ab e ac dividem a. Logo, $c \mid a$. □

Exemplo 4.5. *Sejam* $b = 15$ *e* $c = 14$. *Os dois números são coprimos –* $\mathrm{mdc}\,(a, b) = 1$, *portanto para todo* a, *se* $c \mid ab$ *então* $c \mid a$. *Tomamos como exemplo* $a = 28$*:*

$$c \mid (ab) \quad \text{ou seja,} \quad (\ 14 \mid 28(b)\ ),$$

portanto $c \mid a$, *ou ainda,* $14 \mid 28$ *(sim,* $2(14) = 28$*).* ◀

O Lema de Euclides *Εὐκλείδης*[5][6], a seguir, depende da noção de primalidade, que por ora mencionamos brevemente: *um número natural é primo se somente pode ser dividido por um ou por ele mesmo.*

[5] Euclides (aprox. 300 aEC), Grego.
[6] Esta é a trigésima proposição nos Elementos, de Euclides.

Lema 4.3 (de Euclides)**.** *Se* p *é primo e* $p \mid ab$*, então* $p \mid a$ *ou* $p \mid b$.

Demonstração. Suponha que $p \mid ab$. Se $p \mid a$, o resultado é imediato. Então, suponha que $p \nmid a$, e considere $d = \mathrm{mdc}(a, p)$. Pela definição de MDC, $d \mid p$, portanto d só pode ser 1 ou p. Se $d = p$, então teríamos, pela definição de MDC, $d \mid a$, ou seja, $p \mid a$ – mas já presumimos que $p \nmid a$, portanto $d = \mathrm{mdc}(a, p) = 1$.
Assim, tendo presumido que $p \nmid a$, pelo Teorema 4.6, $p \mid b$. □

Lema 4.4. *Se* $\mathrm{mdc}(a, b) = 1$*, então* $\mathrm{mdc}(a, bc) = \mathrm{mdc}(a, c)$.

A seguir apresentamos duas demonstrações, idênticas exceto por um parágrafo, onde uma delas usa o Lema de Euclides (Lema 4.3[7]) e a outra usa coeficientes de Bézout (Lema 4.2[8]).

Demonstração. (usando o Lema de Euclides). Se $\mathrm{mdc}(a, bc) = 1$ terminamos. Presuma, portanto, que $\mathrm{mdc}(a, bc) > 1$ (ou seja, existe inteiro maior que um, dividindo a e bc).
Seja $d > 1$, tal que $d = \mathrm{mdc}(a, bc)$. Temos que $d \mid a$, e $d \mid bc$.

> Agora, $d \mid a$, por definição. Se $d \nmid b$, teríamos $\mathrm{mdc}(a, b) = d > 1$, que é uma contradição (o enunciado determina que $\mathrm{mdc}(a, b) = 1$). Logo, $d \nmid b$. De acordo com o Lema de Euclides, uma vez que $d \nmid b$ é necessário que $d \mid c$.

Também fica claro que, se algum $e \mid a$ e $e \mid c$, então $e \mid d$ (porque definimos $d = \mathrm{mdc}(a, bc)$), e portanto se houver algum e que divida a e c, ele deve dividir d.
Como $d \mid a$, $d \mid b$, e para todo e, se $e \mid a$ e $e \mid b$, temos $e \mid d$, concluimos que $d = \mathrm{mdc}(a, b)$. □

Demonstração. (usando coeficientes de Bézout). Se $\mathrm{mdc}(a, bc) = 1$ terminamos. Presuma, portanto, que $\mathrm{mdc}(a, bc) > 1$ (ou seja, existe inteiro maior que um, dividindo a e bc).
Seja $d > 1$, tal que $d = \mathrm{mdc}(a, bc)$. Temos que $d \mid a$, e $d \mid bc$.

> *Se dois números multiplicados um pelo outro produzem outro, e se um número primo mede (divide) o número criado a partir deles, então ele também medirá um dos dois números originais.*

No original,

> *Ἐὰν δύο ἀπιθμοὶ πολλαπλασιάσαντες ἀλλήλυς ποιῶσί τινα, τὸν δὲ γενόμενον ἐξ αὐτῶν μετρῇ τις πρῶτος ἀπιθμός, χαὶ ἕνα τῶν ἐξ ἀρχῆς μετρήσει.*
> *(Eán dýo arithmoí pollaplasiásantes allílys poiósí tina, tón dé genómenon ex aftón metrí tis prótos arithmós, chaí éna tón ex archís metrísei.)*

Euclid. **The Elements**. [*S. l.*]: Green Lion Press, 2002. Edição bilíngue Inglês/Grego.

[7] **Lema 4.3 (de Euclides)**: Se p é primo e $p \mid ab$, então $p \mid a$ ou $p \mid b$.
[8] **Lema 4.2 (de Bézout):** Para todos $a, b \in \mathbb{Z}$, $\mathrm{mdc}(a, b)$ é combinação linear inteira de a e b – ou seja, existem $x, y \in \mathbb{Z}$ tais que $\mathrm{mdc}(a, b) = xa + yb$.

Agora, pelo Lema de Bézout, se $\mathrm{mdc}(a, b) = 1$ então existem X, Y, tais que

$$aX + bY = 1$$
$$aXc + bYc = c$$

Como $d \mid a$ e $d \mid bc$, o Lema 4.1 determina que d divide o lado esquerdo. Sendo o lado esquerdo igual ao direito, $d \mid c$.

Também fica claro que, se algum $e \mid a$ e $e \mid c$, então $e \mid d$ (porque definimos $d = \mathrm{mdc}(a, b)$), e portanto se houver algum e que divida a e c, ele deve dividir d.
Como $d \mid a$, $d \mid b$, e para todo e, se $e \mid a$ e $e \mid b$, temos $e \mid d$, concluimos que $d = (a, b)$. □

4.3 Algoritmo de Euclides para cálculo do MDC

Passamos agora ao algoritmo de Euclides, usado para calcular o MDC de dois (ou mais) números[9].
O Lema 4.5 motiva diretamente a construção do algoritmo de Euclides (a demonstração, simples e quase a mesma do Teorema 4.7 (algoritmo de Euclides), é pedida no Exercício 80).

Lema 4.5. *Se $a = bq + r$, então os divisores comuns de a e b são os mesmos que os divisores comuns de b e r. Consequentemente,* $\mathrm{mdc}(a, b) = \mathrm{mdc}(b, r)$.

O algoritmo de Euclides é dado na forma de função recursiva.

[9] Euclides apresentou o algoritmo na proposição 2 do livro sete de sua compilação (o livro *Elementos*) mas, como se deve esperar, há evidências de que o algoritmo era conhecido muito antes de Euclides. A proposição inicia com:

> *Dados dois números não primos entre si, encontrar sua máxima medida.*

O original é:

> *Δῦο ἀριθμῶ δοθέντων μὴ πρώτων πρὸς ἀλλήλους τὸ μέγιστον αὐτῶν αὐτῶν χοινὸν μέτρον εὑρεῖν.*
> *(Dýo arithmó dothénton mí próton prós állílous tó mégiston aftón choinón métron evreín.)*

Euclides formulou suas proposições em termos de medidas, tratando os números como medidas em geometria. Um número "mede" outro se é divisor daquele. A "máxima medida" dos dois números é o maior número que "mede" (em nossa linguagem, "divide") os dois – o MDC.
A proposição seguinte no livro (a de número 3) trata do MDC de três números.

Euclid. **The Elements**. [*S. l.*]: Green Lion Press, 2002. Edição bilíngue Inglês/Grego.

Teorema 4.7 (algoritmo de Euclides)**.** *Sem perda de generalidade, presuma que* $a > b$*, e que* $a = qb + r$*. Então*

$$\operatorname{mdc}(a,b) = \begin{cases} |b| & \text{se } b \mid a \\ \operatorname{mdc}(b,r) & \text{se } b \nmid a \end{cases}$$

Note que usamos o valor absoluto de b, que pode não fazer sentido em qualquer anel (mas é definido em $\mathbb{Z}$).

Demonstração. Começamos pelo primeiro caso, $b \mid a$. Temos também $b \mid b$. Falta mostrar que para todo k, se $k \mid a$ e $k \mid b$, então $k \mid b$ – o que é evidente. No segundo caso, $b \nmid a$, logo $r \neq 0$. Se calcularmos

$$d = \operatorname{mdc}(b,r)$$

temos

(I) $d \mid b$ e $d \mid r$;

(II) se $k \mid b$, $k \mid r$, então $k \mid d$.

Agora analisamos:

(i) de (I), temos $d \mid (qb + r)$, logo $d \mid a$. Também de (I), $d \mid b$;

(ii) suponha que $k \mid a$ e $k \mid b$. Então

$$\begin{aligned} k &\mid (qb + r) \\ kS &= qb + r && \text{(definição de } \mid) \\ kS &= q(kT) + r && (k \mid b) \\ k(S - qkT) &= r \\ k &\mid r && \text{(definição de } \mid) \end{aligned}$$

e portanto, $k \mid a$ e $k \mid b$ implica que $k \mid r$. Mas por (II), se $k \mid b$, $k \mid r$ então $k \mid d$.

Os itens (i) e (ii) acima mostram que $\operatorname{mdc}(b,r)$ será igual a $\operatorname{mdc}(a,b)$. □

Este Teorema nos dá um algoritmo recursivo para calcular o MDC de dois números. No entanto, não está claro que o algoritmo para. O exercício 56 pede esta demonstração. Pode-se usar o fato de que o maior resto possível em cada divisão é menor que no passo anterior, e que não pode haver restos não-inteiros ou não-positivos.

Exemplo 4.6. *Calculamos o MDC de 624 e 162 usando o algoritmo de Euclides.*

$$\begin{aligned}
\operatorname{mdc}(162, 624) &= \operatorname{mdc}(162, 138) && \text{(624 = (3)162+138)}\\
&= \operatorname{mdc}(138, 24) && \text{(162 = (1)138+24)}\\
&= \operatorname{mdc}(24, 18) && \text{(138 = (5)24+18)}\\
&= \operatorname{mdc}(18, 6) && \text{(24 = (1)18+6)}\\
&= 6. && \text{(6|18)}
\end{aligned}$$

O algoritmo precisou de quatro passos. ◄

Teorema 4.8. *A quantidade de iterações do algoritmo de Euclides para cálculo do MDC é finita.*

Há outro algoritmo para cálculo do MDC, que não usa a operação de divisão.

Teorema 4.9. *Para quaisquer* a, b*,*

$$\operatorname{mdc}(a, b) = \begin{cases} |a| & \text{se } a = b \\ \operatorname{mdc}(a\text{-}b, b) & \text{se } a > b \\ \operatorname{mdc}(a, b\text{-}a) & \text{se } a < b \end{cases}$$

Exemplo 4.7. *Calculamos o MDC de 624 e 162 usando o algoritmo com subtrações.*

$$\begin{aligned}
\operatorname{mdc}(162, 624) &= \operatorname{mdc}(162, 624)\\
&= \operatorname{mdc}(162, 462)\\
&= \operatorname{mdc}(162, 300)\\
&= \operatorname{mdc}(138, 24)\\
&= \operatorname{mdc}(114, 24)\\
&= \operatorname{mdc}(90, 24)\\
&= \operatorname{mdc}(66, 24)\\
&= \operatorname{mdc}(42, 24)\\
&= \operatorname{mdc}(18, 24)\\
&= \operatorname{mdc}(18, 6)\\
&= \operatorname{mdc}(12, 6)\\
&= \operatorname{mdc}(6, 6)\\
&= 6.
\end{aligned}$$

◄

4.3.1 Coeficientes de Bézout: algoritmo estendido de Euclides

O Lema 4.2 (Lema de Bézout[10]) afirma que se $\mathrm{mdc}\,(a,b) = d$, então existem inteiros x e y tais que $ax + by = d$. Uma modificação no algoritmo de Euclides para cálculo do MDC pode identificar os coeficientes x e y, como vemos a seguir.

O algoritmo de Euclides pode ser descrito da seguinte forma: iniciando com

$$\begin{aligned} r_0 &= a, \\ r_1 &= b, \end{aligned}$$

calculamos

$$\begin{aligned} r_0 &= q_1 r_1 + r_2 \\ r_1 &= q_2 r_2 + r_3 \\ r_2 &= q_3 r_3 + r_4 \\ &\vdots \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n \\ r_{n-1} &= q_n r_n + 0. \end{aligned}$$

O MDC de a e b (ou seja, o MDC de r_0 e r_1) é r_n.

Podemos usar a penúltima linha para escrever $\mathrm{mdc}\,(a,b) = r_n$ em função de a e b, realizando substituições para trás. Por exemplo, para calcular o MDC de 108 e 33 fazemos

$$\begin{aligned} 108 &= 3(33) + 9 \\ 33 &= 3(9) + 6 \\ 9 &= 1(6) + 3 \\ 6 &= 2(3) + 0 \end{aligned}$$

e concluímos que $\mathrm{mdc}\,(108, 33) = 3$. Queremos os coeficientes de Bézout na equação $108x + 33y = 3$. Notamos que da penúltima linha de nosso cálculo podemos extrair uma expressão do MDC, 3:

$$3 = 9 - 1(6)$$

Continuamos agora, usando as linhas anteriores para expressar 9 e $1(6)$, até

[10] **Lema 4.2 (de Bézout):** Para todos $a, b \in \mathbb{Z}$, $\mathrm{mdc}\,(a,b)$ é combinação linear inteira de a e b – ou seja, existem $x, y \in \mathbb{Z}$ tais que $\mathrm{mdc}\,(a,b) = xa + yb$.

chegarmos a uma expressão de 3 em função de 108 e 33:

$$\begin{aligned}
3 &= 9 - 1(6) \\
&= 108 - 3(33) - 1(6) \\
&= 108 - 3(33) - 1[33 - 3(9)] \\
&= 108 - 3(33) - 33 + 3(9) \\
&= 108 - 4(33) + 3[108 - 3(33)] \\
&= 4(108) - 13(33).
\end{aligned}$$

Os coeficientes de Bézout são 4 e -13:

$$4(108) - 13(33) = 3.$$

No entanto, podemos fazer melhor que isso. Observando o algoritmo de Euclides e o processo de substituição para trás que fizemos, percebemos que sempre podemos escrever o i-ésimo resto, r_i, em função de valores obtidos anterioremente.

$$\begin{aligned}
r_{i-1} &= q r_i + r_{i+1} \\
r_{i+1} &= r_{i-1} - q r_i
\end{aligned}$$

Se tentarmos manter, desde o início, r_i em função de a e b, no final do cálculo teremos os coeficientes de Bézout.

$$\begin{aligned}
r_{i+1} &= r_{i-1} - q_i r_i \\
&= (a x_{i-1} + b y_{i-1}) - q_i (a x_i + b x_i) \\
&= a x_{i-1} - q a x_i + b y_{i-1} - q b y_i \\
&= a(x_{i-1} - q_i x_i) + b(y_{i-1} - q y_i) \\
&= a x_{i+1} + b y_{i+1}
\end{aligned}$$

Então, como $r_{i+1} = a x_{i+1} + b y_{i+1}$, os coeficientes de Bézout na iteração $i+1$ devem ser

$$x_{i+1} = x_{i-1} - q_i x_i \tag{4.2}$$
$$y_{i+1} = y_{i-1} - q_i y_i \tag{4.3}$$

Os valores iniciais de x e y podem ser $x_0 = 1, x_1 = 0$ e $y_1 = 0, y_1 = 1$, porque

$$\begin{aligned}
r_0 &= a = 1a + 0b && (x_0 = 1, y_0 = 0) \\
r_1 &= b = 0a + 1b && (x_1 = 0, y_1 = 1)
\end{aligned}$$

Calculamos o MDC de 48 e 26. No desenvolvimento a seguir, o lado esquerdo

mostra o algoritmo básico de Euclides. O lado direito tem os coeficientes x_i e y_i, que são atualizados conforme as equações 4.2 e 4.3.

r_{i-1}	$= q_i r(i)$	$+ r_{i+1}$	x_i	y_i	i
		48	1	0	0
48	$= 1(26)$	$+ 22$	0	1	1
26	$= 1(22)$	$+ 4$	1	-1	2
22	$= 5(4)$	$+ 2$	-1	2	3
4	$= 2(2)$	$+ 0$	6	-11	4

A última linha tem $r_4 = 2$, que é o MDC de 48 e 26; dali também extraímos os coeficientes de Bézout, $x_4 = 6$ e $y_4 = -11$. Confirmamos:

$$6(48) - 11(26) = 2.$$

Este cálculo pode ser simplificado em uma tabela como a próxima, que mostra o índice das cinco iterações, i, e os valores r_i, q_i, x_i e y_i.

$$\longrightarrow$$

i	0	1	2	3	4	5
r_i	48	26	22	4	2	
q_i		1	1	5	2	
x_i	1	0	1	-1	6	
y_i	0	1	-1	2	-11	

Obtivemos novamente os mesmos coeficientes de Bézout, $x = 6$ e $y = -11$.

4.4 Mínimo Múltiplo Comum

O conceito de mínimo múltiplo comum é simétrico ao de máximo múltiplo comum.

Definição 4.5 (mínimo múltiplo comum)**.** *O* ***mínimo múltiplo comum*** *de* a *e* b*, denotado* $\operatorname{mmc}(a, b)$*, é o menor* m *positivo (exclui-se o zero) que é divisível tanto por* a *como por* b*.* ◀

Excluímos o zero porque de outra forma, ele seria o mínimo múltiplo comum de todos os pares de números: 0 sempre é divisível por a e b, e é o menor natural.

Teorema 4.10. *Sejam* $a > b$ *dois inteiros não negativos. Então*

$$\operatorname{mmc}(a, b) = \begin{cases} a & \text{se } b \mid a \\ \frac{a \operatorname{mmc}(b,r)}{r} & \text{se } a = bq + r, \;\; r > 0 \end{cases}$$

Exemplo 4.8. *O MMC dos inteiros* 15 *e* 20 *é*

$$\begin{aligned}\operatorname{mmc}(15,20) &= 20\operatorname{mmc}(15,5)/5 && (15 \nmid 20)\\ &= (20\cdot 15)/5 && (5 \mid 15)\\ &= 60. && \blacktriangleleft\end{aligned}$$

Assim como o MDC pode ser calculado usando subtrações, o MMC pode ser calculado usando somas.

Teorema 4.11. *Para quaisquer* $a, b \geq 0$*, fixe* $m = a$ *e* $n = b$*. Então*

$$\operatorname{mmc}(a,b) = \begin{cases} a & \text{se } a = b \\ \operatorname{mmc}(a+m,b) & \text{se } a < b \\ \operatorname{mmc}(a,b+n) & \text{se } a > b \end{cases}$$

Exemplo 4.9. *Usando o (entediante) método da soma, verificamos que o MMC dos inteiros* 15 *e* 20 *é*

$$\begin{aligned}\operatorname{mmc}(15,20) &= \operatorname{mmc}(15+15,20)\\ &= \operatorname{mmc}(30,20)\\ &= \operatorname{mmc}(30,20+20)\\ &= \operatorname{mmc}(30,40)\\ &= \operatorname{mmc}(30+15,40)\\ &= \operatorname{mmc}(45,40)\\ &= \operatorname{mmc}(45,40+20)\\ &= \operatorname{mmc}(45,60)\\ &= \operatorname{mmc}(45+15,60)\\ &= \operatorname{mmc}(60,60)\\ &= 60. && \blacktriangleleft\end{aligned}$$

O Teorema 4.12 determina uma relação importante entre o MDC e o MMC de dois números. Sua demonstração é pedida no Exercício 73.

Teorema 4.12. $\operatorname{mmc}(a,b)\operatorname{mdc}(a,b) = |ab|$.

O Teorema 4.12 tem como consequência um algoritmo eficiente para cálculo do MMC:

$$\operatorname{mmc}(a,b) = \frac{|ab|}{\operatorname{mdc}(a,b)}.$$

Isso porque a função recursiva que pode ser obtida a partir do Teorema 4.11[11] opera muito mais passos do que calcular $|ab|/\operatorname{mdc}(a,b)$.

Corolário 4.3. *Se* a *e* b *são co-primos,* $\operatorname{mmc}(a,b) = |ab|$.

Corolário 4.4. *Se* $a > 0$, $\operatorname{mmc}(a, a+1) = a(a+1)$.

Lema 4.6. *O conjunto de múltiplos comuns de dois números naturais positivos* a *e* b *é idêntico ao conjunto dos múltiplos de* $\operatorname{mmc}(a,b)$.

O Teorema 4.13 passa uma clara intuição a respeito dos dois conceitos (MDC e MMC), e da relação entre eles. A demonstração é pedida no Exercício 83.

Teorema 4.13. *Sejam* a *e* b *dois naturais, com fatoração*

$$\begin{aligned} a &= p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}, \\ b &= p_1^{f_1} p_2^{f_2} \dots p_k^{f_k}, \end{aligned}$$

ou seja, os fatores primos de a *são os* p_i*, com expoentes* e_i*, e os de* b *são os mesmos* p_j*, mas com expoentes* f_j*. Então*

$$\begin{aligned} \operatorname{mdc}(a,b) &= \prod_i p_i^{\min(e_i,f_i)}, \\ \operatorname{mmc}(a,b) &= \prod_i p_i^{\max(e_i,f_i)}. \end{aligned}$$

Exemplo 4.10. *Sejam*

$$\begin{aligned} a &= 2^3 3^2 5^0 7^1 = 504 \\ b &= 2^2 3^1 5^1 7^2 = 2940 \end{aligned}$$

Então,

$$\begin{aligned} \operatorname{mdc}(a,b) &= \prod_i p_i^{\min(e_i,f_i)} \\ &= 2^2 3^1 5^0 7^1 \\ &= 84. \end{aligned}$$

[11] **Teorema 4.11:** Para quaisquer $a, b \geq 0$, fixe $m = a$ e $n = b$. Então

$$\operatorname{mmc}(a,b) = \begin{cases} a & \text{se } a = b \\ \operatorname{mmc}(a+m,b) & \text{se } a < b \\ \operatorname{mmc}(a,b+n) & \text{se } a > b \end{cases}$$

$$\begin{aligned}\operatorname{mmc}(a,b) &= \prod_i p_i^{\max(e_i,f_i)} \\ &= 2^3 3^2 5^1 7^2 \\ &= 17640.\end{aligned}$$ ◀

4.5 Números de Fibonacci

A chamada "sequência de Fibonacci" é uma sequência definida recursivamente, descrevendo um fenômeno de crescimento populacional. É conhecida por ter sido descrita por Fibonacci[12] (ou "Leonardo de Pisa"[13]) em 1202, em seu "Liber Abaci", e de outras maneiras na Grécia e Índia. A alegoria de Fibonacci consistia em coelhos que se reproduziam de maneira cadenciada, mês a mês, sem nunca morrer. Presume-se que há inicialmente um casal de coelhos, e que cada casal fica pronto para reprodução em dois meses. A cada mês, cada casal produz um novo casal[14]. A sequência de números dando as quantidades de casais em cada mês é a chamada *sequência de Fibonacci*, embora tenha sido conhecida na Índia, antes de Fibonacci nascer[15]

[12] Leonardo Fibonacci (1170-1250), nascido na República de Pisa (Hoje Itália).

[13] O primeiro nome é Leonardo (ou "Lionardo", na grafia da época). Outros nomes aparecem, mas não há certeza sobre a natureza ou origem deles (Leonardo Bigollo, Leonardo Pisano, Leonardo Bonacci, ou ainda, "Fibonacci", possivelmente significando "filho de Bonacci"). Ë mais comum a referencia a "Leonardo de Pisa", ou "Leonardo Pisano" – ele nasceu na República de Pisa.

[14] O fato da descrição usar coelhos e presumir que nunca morrem garante a denominação alternativa "coelhos imortais de Fibonacci". Este livro parece ter sido o primeiro a introduzir a notação posicional com base dez e os numerais arábicos na Europa. A obra foi publicada inicialmente em 1202,em Latim, mas não há cópia escrita dessa edição. Uma nova edição, de 1227 traz, no Capítulo doze, o problema:

> *Um certo homem tinha um casal de coelhos juntos em un certo lugar fechado, e queremos saber quantos são criados desse casal em um ano quando é da natureza deles em um mês gerar um novo casal, e no segundo mês esses que nasceram gerarem outros também. (...)*
> *Você pode de fato ver na margem como operamos, que somamos o primeiro número ao segundo, 1 ao 2, e o segundo ao terceiro, e o terceiro ao quarto, e o quarto ao quinto, e assim um após o outro até termos adicionado o décimo ao décimo primeiro, 144 a 233, e tivemos a soma de coelhos acima, 377, e assim você pode encontrá-la para um número sem fim de meses.*

O original em Latim não é incluído pode ser de difícil acesso. Há uma tradução para o Inglês.

Sigler, Laurence. **Liber Abaci: A Translation into Modern English of Leonardo Pisano's Book of Calculation**. [*S. l.*]: Springer, 2002.

[15] A sequência de Fibonacci e o método para formá-la foram descritos entre os anos 600 e 800 na Índia por Virahāṅka (विरहाङ्क), além de outros, antes do nascimento de Fibonacci.

Singh, Paramand. The So-called Fibonacci Numbers in Ancient and Medieval India. **Historia Mathematica**, v. 12, n. 3, p. 229–244, 1985.

Definição 4.6 (número de Fibonacci)**.** *Seja uma sequência* (u_n) *definida da seguinte maneira*[16]*:*

$$\begin{aligned} u_1 &= 1, \\ u_2 &= 1, \\ u_n &= u_{n-1} + u_{n-2}. \end{aligned}$$

Os u_n *são chamados de* ***números de Fibonacci****, e a sequência* (u_n) *é chamada de* ***sequência de Fibonacci****.* ◀

O Lemma 4.7 é útil nos momentos em que precisamos usar números de Fibonacci com índices negativos. Basicamente, o Lema diz que é possível "retroceder" a sequência de Fibonacci, e dá uma forma fechada para a sequência estendida.

Lema 4.7. *A extensão da sequência de Fibonacci para* $\mathbb{Z}$ *resulta em* $u_{(-n)} = (-1)^{n+1}u_n$.

Lema 4.8. $u_{m(k+1)} = u_{mk+m}$,

Demonstração. Por indução em m. □

Números de Fibonacci podem ser descritos por uma forma fechada, usando a razão áurea, através da fórmula de Euler-Binet.

Definição 4.7 (razão áurea)**.** *Denotamos por* ϕ *a* ***razão áurea****, solução positiva da equação* $x^2 - x - 1 = 0$*:*

$$\phi = \frac{1+\sqrt{5}}{2}.$$

A segunda raiz da equação é negativa, e denotada $\hat{\phi}$*:*

$$\hat{\phi} = \frac{1-\sqrt{5}}{2}.$$ ◀

Teorema 4.14 (fórmula de Euler-Binet)**.** *Seja* ϕ *a razão áurea, e*

$$\hat{\phi} = 1 - \phi = -\frac{1}{\phi}.$$

Então

$$u_n = \frac{\phi^n - \hat{\phi}^n}{\sqrt{5}}.$$

[16] Alguns autores definem de forma alternativa, mas equivalente: $u_0 = 0$; $u_1 = 1$; $u_n = u_{n-1} + u_{n-2}$.

Demonstração. Para a base, usamos u_0 e u_1:

$$\begin{aligned}
\frac{\phi^0 - \hat{\phi}^0}{\sqrt{5}} &= \frac{1-1}{\sqrt{5}} = u_0 \\
\frac{\phi^1 - \hat{\phi}^1}{\sqrt{5}} &= \frac{\phi - \hat{\phi}}{\sqrt{5}} \\
&= \frac{\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}}{\sqrt{5}} \\
&= 1 = u_1
\end{aligned}$$

A hipótese de indução é: para todo $i < n$,

$$\begin{aligned}
u_i &= \frac{\phi^i - \hat{\phi}^i}{\sqrt{5}}, \quad \text{ou} \\
u_i\sqrt{5} &= \phi^i - \hat{\phi}^i.
\end{aligned}$$

Precedemos ao passo. Como tanto ϕ como $\hat{\phi}$ são soluções de $x^2 - x - 1 = 0$, então

$$\begin{aligned}
\phi^2 &= 1 + \phi, \\
\hat{\phi}^2 &= 1 + \hat{\phi}.
\end{aligned}$$

Agora verificamos que

$$\begin{aligned}
\phi^n - \hat{\phi}^n &= \phi^2\phi^{n-2} - \hat{\phi}^2\hat{\phi}^{n-2} \\
&= (1+\phi)\phi^{n-2} - (1+\hat{\phi})\hat{\phi}^{n-2} \\
&= \phi^{n-2} + \phi^{n-1} - \hat{\phi}^{n-2} - \hat{\phi}^{n-1} \\
&= \left(\phi^{n-2} - \hat{\phi}^{n-2}\right) + \left(\phi^{n-1} - \hat{\phi}^{n-1}\right) \\
&= (u_{n-2} + u_{n-1})\sqrt{5} \qquad \text{(hipótese de indução)} \\
&= u_n\sqrt{5},
\end{aligned}$$

e $u_n = \left(\phi^n - \hat{\phi}^n\right)/\sqrt{5}$. □

Seguem demonstrações de diversas propriedades de números de Fibonacci. Dois números consecutivos de Fibonacci são coprimos.

Teorema 4.15. $\mathrm{mdc}\,(u_n, u_{n+1}) = 1$.

Demonstração. Por indução em n.
A base é, trivialmente, com $n = 1$, já que $\mathrm{mdc}\,(u_1, u_2) = 1$.
A hipótese de indução é $\mathrm{mdc}\,(u_n, u_{n\text{-}1}) = 1$.

O passo é muito simples,

$$\begin{aligned}\operatorname{mdc}(u_{n+1}, u_n) &= \operatorname{mdc}(u_n + u_{n\text{-}1}, u_n)\\ &= \operatorname{mdc}(u_{n\text{-}1}, u_n)\\ &= 1, \qquad \text{(pela hipótese de indução)}\end{aligned}$$

finalizando a demonstração. □

O Lema 4.9 é bastante útil, e o Exercício 63 pede duas demonstrações diferentes dele.

Lema 4.9. *Se* $m \mid n$*, então* $u_m \mid u_n$.

O Lema 4.10 determina uma propriedade simples de números de Fibonacci. Sua demonstração é bastante simples, e é pedida no Exercício 64

Lema 4.10. *Se* $m, n \geq 1$*,* $u_m \mid u_{mn}$.

A igualdade de Honsberger será útil na demonstração de um Teorema a respeito do MDC de números de Fibonacci.

Lema 4.11 (igualdade de Honsberger)**.** $u_{m+n} = u_m u_{n+1} + u_{m-1} u_n$.

Demonstração. Por indução em n.
Para a base, fixamos m, e verificamos, para $n = 1$ e $n = 2$ que:

$$\begin{aligned}u_m u_{n+1} + u_{m-1} u_n &= u_m u_{1+1} + u_{m-1} u_1\\ &= u_m(1) + u_{m-1}(1) \qquad (u_1 = 1, u_2 = 1)\\ &= u_m + u_{m-1}\\ &= u_{m+1}\\ &= u_{m+n}.\end{aligned}$$

$$\begin{aligned}u_m u_{n+1} + u_{m-1} u_n &= u_m u_{2+1} + u_{m-1} u_2\\ &= u_m(2) + u_{m-1}(1) \qquad (u_2 = 1, u_3 = 2)\\ &= u_m + u_m + u_{m-1}\\ &= u_m + u_{m+1}\\ &= u_{m+2}\\ &= u_{m+n}.\end{aligned}$$

A base é dupla, porque durante o passo usaremos a hipótese duas vezes, uma usando n e outra usando $n - 1$, e a validade do passo depende da validade da afirmação para *dois* valores anteriores.

A hipótese de indução, para $n-1$ e n, é

$$u_{m+n-1} = u_m u_n + u_{m-1} u_{n-1}, \tag{4.4}$$
$$u_{m+n} = u_m u_{n+1} + u_{m-1} u_n. \tag{4.5}$$

$$\begin{aligned}
u_{m+(n+1)} &= u_{m+n} + u_{m+n-1} \\
&= u_{m+n} + (u_m u_n + u_{m-1} u_{n-1}) && \text{(por 4.4)} \\
&= (u_m u_{n+1} + u_{m-1} u_n) + (u_m u_n + u_{m-1} u_{n-1}) && \text{(por 4.5)} \\
&= u_m (u_{n+1} + u_n) + u_{m-1} (u_n + u_{n-1}) \\
&= u_{m-1} u_{n+1} + u_m u_{n+1}. && \square
\end{aligned}$$

Teorema 4.16. $\operatorname{mdc}(u_m, u_n) = u_{\operatorname{mdc}(m,n)}$.

Demonstração. (usando o algoritmo de Euclides) Presumimos, sem perda de generalidade, que $n \geq m$. Então sejam q, r o quociente e o resto da divisão de n por m:

$$n = qm + r, \quad 0 \leq r < m.$$

Então

$$\begin{aligned}
\operatorname{mdc}(u_m, u_n) &= \operatorname{mdc}(u_m, u_{mq+1} u_r + u_{qm} u_{r\text{-}1}) \\
&\qquad \text{(igualdade de Honsberger 4.11)} \\
&= \operatorname{mdc}(u_m, u_{qm+1} u_r) && (u_m \mid u_{qm}) \\
&= \operatorname{mdc}(u_m, u_r). && (u_m \nmid u_{qm+1}, \text{Teorema 4.15}) \\
&\qquad \text{(também } (a, bc) = (a, b), \text{ Lema 4.4)}
\end{aligned}$$

Se, neste processo, olharmos *apenas para os índices* (que seria como substituir $u_m \to m$, $u_n \to n$, $u_q \to q$, $u_r \to r$), perceberemos que esses índices se comportam como em iterações do algoritmo de Euclides, que eventualmente terminará com o último resto igual ao MDC dos dois números: haverá um passo em que

$$\operatorname{mdc}(u_a, u_b) = \operatorname{mdc}(u_d, u_0),$$

mas $u_0 = 0$ (pela definição de números de Fibonacci), e

$$\operatorname{mdc}(u_m, u_n) = \operatorname{mdc}(u_d, 0) = u_d = u_{\operatorname{mdc}(m,n)}. \qquad \square$$

Demonstração. (usando o Lema de Bézout) Seja $d = \operatorname{mdc}(m, n)$.
Para que $\operatorname{mdc}(()\, u_m, u_n) = u_d$, pela definição de MDC é necessário que

i) $u_d \mid u_m, u_d \mid u_n$

ii) se $u_e \mid u_m, e \mid u_n$, então $u_e \mid u_d$.

Mas sabemos que $d \mid m$ e $d \mid n$, e também, pelo Teorema 4.9[17], que isso implica que (i) é verdade.
Para provar (ii), apontamos que pelo Lema de Bézout existem $x, y \in \mathbb{Z}$ tais que $d = mx + ny$ (porque d é $\mathrm{mdc}(m, n)$).
Como $u_m \mid u_{mx}$ (Lema 4.10), então $e \mid u_m$ implica que $e \mid mx$. Da mesma forma, $e \mid midny$. Mas pela igualdade de Honsberger (Lema 4.11),

$$u_{m+n} = u_m u_{n+1} + u_{m-1} u_n,$$

e portanto

$$e \mid u_{mx-1} u_{ny} + u_{mx} u_{ny+1}$$

e

$$e \mid u_{mx+ny}. \qquad \square$$

A demonstração do Teorema 4.17 é tema do Exercício 65. A representação de inteiros como soma de quadrados é, por si mesma, tópico suficientemente relevante para merecer um capítulo inteiro (o Capítulo 10 trata exclusivamente da representação de inteiros como soma de dois, três ou quatro quadrados).

Teorema 4.17. $u_{2n+1} = u_n^2 + u_{n+1}^2$.

Teorema 4.18. $2 \mid u_n$ *se e somente se* $3 \mid n$.

Demonstração. A demonstração é extremamente simples, por indução em n, com passo de três em três.
A base é $2 \nmid u_1 = 1$; $2 \nmid u_2 = 1$; $2 \mid u_3 = 2$.
Por hipótese, suponha que o enunciado valha para todo u_i anterior a u_n. Então, se $3 \mid k$, temos

$$\begin{aligned}
2 \mid u_k &= u_{k-1} + u_{k-2}, && \text{(ímpar + ímpar)} \\
2 \nmid u_{k+1} &= u_k + u_{k-1}, && \text{(par + ímpar)} \\
2 \nmid u_{k+2} &= u_{k+1} + u_k, && \text{(ímpar + par)}
\end{aligned}$$

E o Teorema está demonstrado. $\square$

4.5.1 Complexidade[18] do algoritmo de Euclides

A sequência de Fibonacci pode ser usada para determinar a complexidade do algoritmo de Euclides. Nesta Seção o limite (no Teorema 4.19) não é o

[17] **Lema 4.9:** Se $m \mid n$, então $u_m \mid u_n$.

[18] A "Complexidade de tempo" do algoritmo é uma medida de crescimento assintótico da quantidade de operaçõs do algoritmo, a partir do "tamanho da entrada" (neste caso os números a dividir). É usualmente expressa usando notação assintótica, "O, Θ, Ω". Neste texto apenas um limite superior é determinado – que implica que a complexidade é $O(\log(a))$ – mas a descrição assintótica é deixada de lado.

mais justo possível, mas resulta em demonstração ligeiramente mais simples (que é pedida nos Exercícios 68 e 69).

Lema 4.12. *Sejam* a *e* b*, com* $a > b$*. Então existem* q, r *tais que*

$$a = qb + r.$$

O algoritmo de Euclides, quando aplicado para obter q *e* r*, necessita de uma quantidade de passos* k *tal que*

$$a \geq u_{k+1},$$
$$b \geq u_k.$$

O Lema é simples, e deriva do seguinte fato: renomeando as variáveis no algoritmo com $r_0 = a$ e $r1 = b$, os "restos" (variáveis r_i) são

$$r_0 = a \geq r1 = b \geq r2 \geq \ldots \geq r_k \geq 1,$$

com

$$r_{i-2} = q_i r_{i-1} + r_i, \quad q_i \geq 1$$

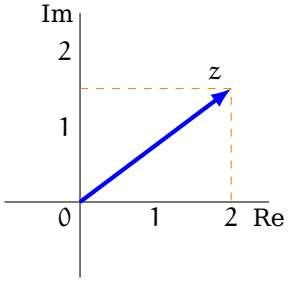
par todo $i > 1$.
Usando o Lema 4.12 e a fórmula de Euler-Binet (Teorema 4.14) é possível demonstrar o Teorema 4.19, que determina a complexidade do algoritmo de Euclides.

Teorema 4.19. *O número de iterações do algoritmo de Euclides quando* $a \geq b \geq 0$ *é* k*, tal que*

$$k < \frac{5}{2} \log a + \frac{3}{2}.$$

4.6 Domínios Euclideanos: Inteiros Gaussianos e Polinômios

A demonstração do Teorema da divisão depende de uma relação de ordem (escolhemos o "menor positivo" dentre os números $a - qb$). Em anéis sem ordem total, a demonstração não é válida. Ainda assim, podemos determinar uma ordem parcial em um anel não-ordenado, de forma a tentar obter resultado semelhante.
Identificamos cada número complexo $a+bi$ com o vetor (a, b) em $\mathbb{R}^2$. Assim, a projeção de um vetor (número complexo) no eixo das abscissas identifica a parte real do número; a projeção no eixo das ordenadas identifica a parte imaginária. Damos a este plano o nome de *plano complexo*. A figura a seguir mostra a representação do número $z = 2 + (3/2)i$.



Teorema 4.20. *A multiplicação de um complexo por* i *resulta em rotação de sua representação no plano por um ângulo de* $\pi/2$.

Demonstração. Usando coordenadas polares, um complexo $re^{i\theta}$, com raio r e ângulo θ no plano. Assim, $i = (1)e^{i(\pi/2)}$, e

$$r_1 e^{i\theta_1} r_2 e^{i\theta_2} = r_1 r_2 e^{i(\theta_1+\theta_2)},$$

logo

$$\begin{aligned} i\left(re^{i\theta}\right) &= e^{i(\pi/2)}\left(re^{i\theta}\right) \\ &= re^{i(\theta+\pi/2)}. \end{aligned}$$

□

Nada dissemos sobre o efeito sobre a *norma*, porque não usamos norma euclideana, como será esclarecido adiante.
Usaremos, a partir de agora, *inteiros Gaussianos*[19].

Definição 4.8 (inteiros Gaussianos)**.** *Os* ***inteiros Gaussianos****, denotados* $\mathbb{Z}[i]$*, são as combinações lineares inteiras de* 1 *e* i*, ou seja, números da forma* $a + bi$ *onde* a *e* b *são inteiros e* $i^2 = -1$. ◀

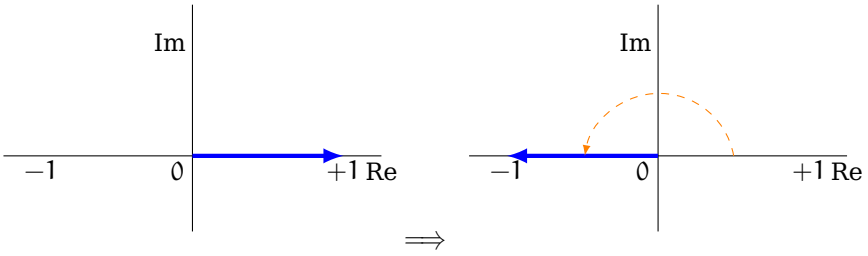
Ainda que saibamos que pela definição de número complexo $i^2 = -1$, é interessante observar que, conforme demonstramos no Teorema 4.20, a multiplicação por i é uma rotação por ângulo igual a $\pi/2$. E realmente, o complexo $1 + 0i$, quando multiplicado duas vezes por i resulta no complexo $-1 + 0i$:

$$(1) \cdot (i) \cdot (i) = -1.$$

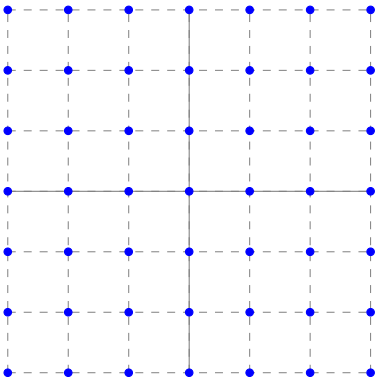
[19] Quando estava estudando a Lei da Reciprocidade Biquadrática, Gauss percebeu que o teorema e a demonstração seriam mais facilmente descritos usando números do tipo "número complexo inteiro" (*numerum integrum complexum* é o termo usado) do que trabalhando diretamente com números inteiros.

Gauss, Johannes Carl Friedrich. Theoria residuorum biquadraticorum. Commentatio secunda. **Comm. Soc. Reg. Sci. Göttingen**, v. 7, p. 89–148, 1831.

A "Lei da Reciprocidade Biquadrática" estabelece uma relação entre a solubilidade de duas equações, $x^4 - p = Kq$ e $x^4 - q = Kp$, que são denotadas "$x^4 \equiv p \pmod{q}$" e "$x^4 \equiv q \pmod{p}$". Esta notação é introduzida no Capítulo **??** deste texto, mas a reciprocidade biquadrática, não.



Os inteiros Gaussianos são um anel, subconjunto de $\mathbb{C}$ (ou seja, um subanel). No plano complexo, ocupam as coordenadas inteiras.



A noção de divisibilidade em $\mathbb{Z}[i]$ é a mesma para qualquer anel – podemos manter a definição que já temos. Daremos, no entanto, alguns exemplos.

- $-i \mid (-1-2i)$, porque $-i(2-i) = -1-2i$;
- $4-12i \mid 20-20i$, porque $(2+i)(4-12i) = 20-20i$;
- $(3-5i) \nmid (1-i)$, porque $(3-5i)/(1-i) = 11/2+5i/2$, que não tem coeficientes inteiros, e portanto não está em $\mathbb{Z}[i]$.

Claramente, um inteiro n divide um inteiro Gaussiano $a+bi$ se e somente se $n \mid a$ e $n \mid b$.

Definição 4.9 (norma)**.** *Definimos* ***norma***[20] *para números complexos como* $N(a+bi) = a^2+b^2$. ◀

Exemplo 4.11. *A norma de* $-3+4i$ *é* $(-3)^2+(4)^2 = 9+16 = 25$. ◀

[20] Usualmente, para vetores em $\mathbb{R}^2$ e para números complexos, define-se a norma como $\sqrt{a^2+b^2}$, *para que o valor da norma coincida com a distância da origem até o ponto associado ao vetor.* No entanto, em Teoria de Números é mais importante *que a norma seja um valor inteiro* – daí a ausência da raiz quadrada.

Teorema 4.21. *A norma para inteiros Gaussianos é multiplicativa:* $N(\alpha\beta) = N(\alpha)N(\beta)$.

A verificação deste Teorema, pedida no exercício 85, consiste de simples manipulação de fórmulas, sem passos não-triviais.

Exemplo 4.12. *Sejam* $z = -3 + 4i$ *e* $w = 2 - 8i$. *Então* $zw = 26 + 32i$.

$$\begin{aligned} N(-3+4i) &= (-3)^2 + (4)^2 = 9 + 16 = 25 \\ N(2-8i) &= (2)^2 + (-8)^2 = 68 \\ N(zw) &= N(26+32i) \\ &= 26^2 + 32^2 \\ &= 1700 \\ &= (25)(68) \\ &= N(z)N(w). \end{aligned}$$ ◀

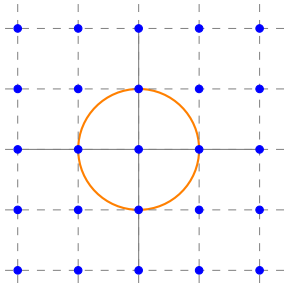
Corolário 4.5. *Há exatamente quatro unidades no anel dos inteiros Gaussianos:* ± 1 *e* $\pm i$.

Demonstração. Da multiplicatividade da norma: para que $\alpha\beta = 1$, é necessário que $N(\alpha)N(\beta) = N(1)$, e como $N(1) = 1$, α e β devem ter norma um. Assim,

$$\begin{aligned} (1)(1) &= 1, \\ (-1)(-1) &= 1, \\ (-i)(i) &= 1. \end{aligned}$$

E temos os inversos $1^{-1} = 1$; $(-1)^{-1} = -1$; e $i^{-1} = -i$. □

As unidades – que tem norma um – são os vetores com coordenadas inteiras no círculo unitário no plano complexo, já que a norma é[21] $a^2 + b^2$.



[21] Para outros valores, a norma *não* é a distância até a origem, porque abrimos mão da norma Euclideana!

Teorema 4.22. *$\alpha\overline{\alpha} = N(\alpha)$, para todo inteiro Gaussiano α, onde $\overline{\alpha}$ é o conjugado complexo de α.*

Exemplo 4.13. *Seja $z = -2 + 5i$. A norma de z é $N(z) = (-2)^2 + 5^2 = 29$ Então*

$$\begin{aligned} z\overline{z} &= (-2+5i)(-2-5i) \\ &= 4 - 25i^2 \\ &= 29 \\ &= N(z). \end{aligned}$$ ◀

A demostração do teorema da divisão não pode ser usada para inteiros Gaussianos, porque nela escrevemos os elementos da forma "$a + kb$", e escolhemos o resto r como o *menor positivo* dentre eles. Não há o conceito de "menor positivo" em $\mathbb{Z}[i]$.
A norma em $\mathbb{Z}[i]$ poderá ser útil, mas precisamos de cuidado: nos inteiros podemos contar com $a \mid b \Rightarrow -a \mid b$, mas isto não é válido para norma de inteiros Gaussianos. Como exemplo: $-2 \mid 10$ e $5 \mid -25$ nos inteiros. Mas em $\mathbb{Z}[i]$, tanto $2-3i$ como $2+3i$ tem norma 13, mas nenhum divide o outro: Os múltiplos de $2-3i$ com a mesma norma são

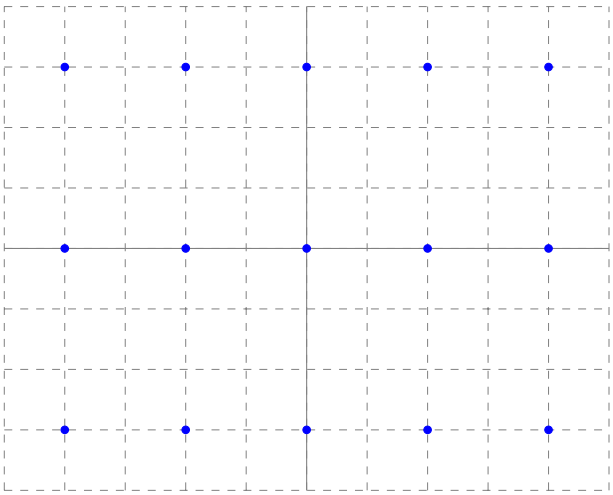
$$\begin{aligned} (1)(2-3i) &= 2-3i \\ (-1)(2-3i) &= -2+3i \\ (i)(2-3i) &= 3+2i \\ (-i)(2-3i) &= -3-2i \end{aligned}$$

e $2+3i$ não está entre eles! Ou seja, se dois números α e β tem a mesma norma, não necessariamente diferem por multiplicação por unidade ($\alpha = \pm\beta$ ou $\alpha \pm i\beta$). Tomar a norma de um inteiro Gaussiano tem efeito maior sobre um número do que tomar o valor absoluto de um número inteiro.
No entanto, podemos demonstrar um resultado para inteiros Gaussianos que é análogo ao Teorema da Divisão para $\mathbb{Z}$ (e anéis ordenados).

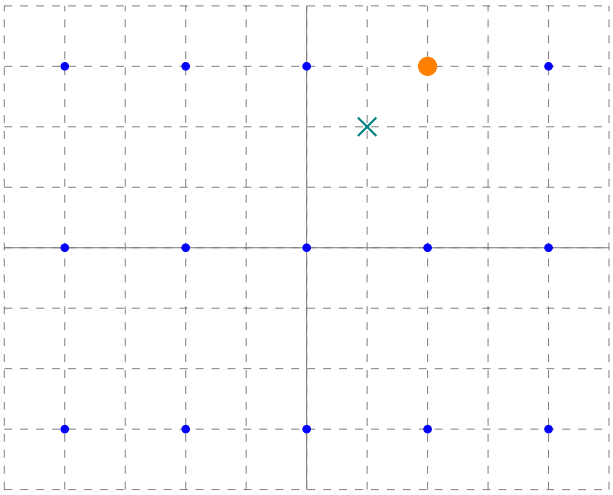
Teorema 4.23. *Sejam $\alpha, \beta \in \mathbb{Z}[i]$, com $\beta \neq 0$. Então existem $\gamma, \rho \in \mathbb{Z}[i]$ tais que $\alpha = \gamma\beta + \rho$, tal que $N(\rho) < N(\beta)$.*

Claramente, γ e ρ são quociente e resto no enunciado do Teorema.

Demonstração. (informal)
Os múltiplos do inteiro gaussiano β formam um reticulado, que podemos visualizar como infinitos retângulos. Se $\beta = a+bi$, os lados destes retângulos tem comprimento a e b. A figura a seguir mostra os múltiplos de um inteiro Gaussiano β $(2+3i)$.



O inteiro Gaussiano α tem coordenadas inteiras, mas não necessariamente no reticulado gerado por β. Identificamos no reticulado de β um ponto mais próximo de α, e como este ponto está no reticulado de β, ele representa um ponto $\gamma\beta$. A figura a seguir ilustra a divisão de $1+2i$ por $2+3i$.



O ponto $\beta = 2+3i$ é representado por um círculo, e $\alpha = 1+2i$ por uma cruz. Note que pode haver mais de um ponto mais próximo. de α.

Temos α é $\gamma\beta + \rho$, onde ρ é, também, inteiro Gaussiano.

Resta mostrar que $N(\rho) < N(\beta)$. Se $\beta = a + bi$ e $\rho = x + yi$, temos $x \leq a/2$

e $y \leq b/2$, logo

$$\begin{aligned} N(\rho) &= x^2 + y^2 \\ &\leq \left(\frac{a}{2}\right)^2 + \left(\frac{b}{2}\right)^2 \\ &= \frac{a^2}{4} + \frac{b^2}{4} \\ &= \frac{N(\beta)}{4}. \end{aligned}$$

□

Corolário 4.6. *Podemos realizar algo semelhante a divisão em $\mathbb{Z}[i]$ de maneira simples usando aritmética racional: para dividir $\alpha = a + bi$ por $\beta = c + di$, calculamos os inteiros mais próximos de a/c e d/b:*

$$\begin{aligned} a + bi \div c + di &= q(c + di) + r \\ q &= \left\lfloor \frac{a}{c} \right\rceil + \left\lfloor \frac{b}{d} \right\rceil \\ r &= \alpha - q\beta, \end{aligned}$$

onde $\lfloor x \rceil$ é o inteiro mais próximo de x. O resultado não é necessariamente único, e o resto pode ser negativo.

O que fizemos com os inteiros Gaussianos foi usar uma norma que nos permitiu usar o algoritmo de Euclides. O mesmo algoritmo funcionará em qualquer anel que, mesmo não sendo totalmente ordenado, admita uma função λ com papel semelhante a esta norma, para que possamos definir a divisão como $a = qb + r$, com $\lambda(r)$ menor que $\lambda(b)$. Isto é a definição de um *domínio Euclideano* – que é, informalmente, um anel onde é possível usar o algoritmo de Euclides.

Definição 4.10 (domínio Euclideano)**.** *Um **domínio Euclideano** é um anel comutativo R onde se pode definir uma função $\lambda : R \setminus \{0\} \to \mathbb{N}$, tal que para todos $a, b \in R$, com b não nulo,*

(i) $\lambda(a) \leq \lambda(ab)$

(ii) existem $q, r \in R$, com $a = qb + r$, tais que $r = 0$ ou $\lambda(r) < \lambda(b)$.

*A função λ é uma **norma** neste domínio Euclideano.* ◄

O zero foi excluído do domínio da norma porque preferimos fixar $\lambda(0) = 0$ (e a norma de zero não pode ser diferente de zero).
Dizemos que λ é *uma* norma, porque não é única. A propriedade (ii) diz essencialmente que vale o algoritmo da divisão, mas não há a necessidade de q e r serem únicos.

Além dos inteiros Gaussianos, o anel $\mathbb{R}[x]$ pode ser tratado como Domínio Euclideano, se usarmos uma norma apropriada.

Exemplo 4.14. *O anel $\mathbb{R}[x]$ é domínio Euclideano, se tomarmos $\lambda(p)$ dando o grau do polinômio: $\lambda(2x^3 - 4x + 10) = 3$. Claramente, (i) vale, porque o grau do polinômio st é o produto dos graus de s e t. (ii), o algoritmo da divisão também vale para polinômios em uma variável, e a divisão de um polinômio de grau s por outro sempre resultará em resto com grau menor que o do polinômio divisor.* ◀

Uma vez que tenhamos o algoritmo da divisão, podemos usar o algoritmo de Euclides para computar máximos divisores comuns.

Teorema 4.24. *Em todo domínio Euclideano[22], é possível calcular algum máximo divisor comum para quaisquer dois elementos.*

A demonstração do Teorema 4.24 é a mesma da existência do MDC para inteiros, exceto que não podemos garantir unicidade do MDC em domínios Euclideanos (e é este o motivo do uso da palavra "algum" ao invés de "o" no enunciado).
Em domínios Euclideanos, vale também o Lema de Bézout (4.2), que determina que o MDC de dois elementos é combinação linear inteira deles.

Exemplo 4.15. *Em $\mathbb{R}[x]$, procuramos $\operatorname{mdc}\left(x^2, x^3\right)$. O MDC não é x, que divide tanto x^2 como x^3, porque $x \mid x^2$, e x^2 também divide ambos. Também não é somente "x^2", porque os múltiplos de x^2 também são:*

$$\left(\frac{1}{k}\right) kx^2 = x^2, \qquad (kx^2 \mid x^2)$$

$$\left(\frac{x}{k}\right) kx^2 = x^3. \qquad (kx^2 \mid x^3)$$

Isso acontece porque a ordem que impusemos em $\mathbb{R}[x]$ é parcial, e não total: dois polinômios de mesmo grau podem ter diferentes coeficientes na variável de mais alta potência.
Ainda em $\mathbb{R}[x]$, $\operatorname{mdc}\left(x^3\text{-}x^2, x^2\text{-}1\right)$ contém todos os múltiplos do polinômio $x-1$: para todo k,

$$\left(\frac{x^2}{k}\right)\Big(k(x-1)\Big) = x^3 - x^2, \qquad (k(x-1) \mid x^3 - x^2)$$

$$\left(\frac{x+1}{k}\right)\Big(k(x-1)\Big) = x^2 - 1. \qquad (k(x-1) \mid x^2 - 1)$$

No entanto, a não ser por multiplicação por constante, o MDC de polinômios em $\mathbb{R}[x]$ é único. ◀

[22] Na verdade, pode-se definir MDCs em estruturas mais gerais que domínios Euclideanos, mas não tratamos disso.

É interessante que uma tentativa de usar "tanto o grau do polinômio como o coeficiente líder" levaria a uma situação semelhante à de $\mathbb{C}$, onde essencialmente estaríamos tentando obter ordem total para o produto cartesiano de dois conjuntos infinitos ordenados ($\mathbb{R} \times \mathbb{R}$ para complexos, $\mathbb{Z} \times \mathbb{R}$ para $\mathbb{R}[x]$, porque o grau é inteiro e o coeficiente líder é real) – estas relações de ordem, no entanto, não existem.

Retomando o MDC para inteiros, observamos que temos na definição uma exigência de que o MDC de dois números seja positivo. Esta restrição garante a unicidade do MDC – de outra forma, teríamos $\operatorname{mdc}(8, 12) = \pm 4$, já que $\pm 4 \mid 8$, $\pm 4 \mid 12$, e se houver algum c que divida 8 e 12, (por exemplo, 2) então $c \mid \pm 4$.

Exercícios

Ex. 41 — Prove que, quando restrita a inteiros não-negativos, "divide" ($\mid$) é uma relação de ordem. Explique o que acontece se incluirmos os negativos.

Ex. 42 — Mostre que para qualquer inteiro não negativo n, o número $n(2n+1)(n+1)/6$ é inteiro.

Ex. 43 — Mostre que se $7 \mid (a^2 + b^2)$, então $7 \mid a$ e $7 \mid b$.

Ex. 44 — Mostre que para todo n,

(a) $3 \mid (10^n - 7^n)$

(b) $9 \mid (10^n - 1)$

(c) $8 \mid (3^{2n} + 7)$

(d) $14 \mid 3^{4n+2} + 5^{2n+1}$

Ex. 45 — Mostre que, para todos $n, k \in \mathbb{N}$, com $n > k$, $(n + k)!/(n - k)!$ é divisível por $2k$.

Ex. 46 — Mostre que todo quadrado é da forma $3k$ ou $3k + 1$.

Ex. 47 — Mostre que todo cubo é da forma $9k$ ou $9k + 1$ ou $9k + 8$.

Ex. 48 — Prove que todo racional pode ser escrito como soma de frações onde o numerador é um.

Ex. 49 — Mostre que todo número natural tem algum múltiplo positivo que, quando escrito na base dez, tem somente dígitos um e zero.

Ex. 50 — O Exemplo 2.19[23] apresentou o corpo das matrizes quadradas da forma

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix},$$

com $a, b \in \mathbb{Q}$ (ou $a, b \in \mathbb{R}$), com determinante não nulo. (É um corpo porque além de ser um anel, nele a multiplicação é comutativa e toda matriz tem inversa). Prove que com $a, b \in \mathbb{Z}$ a estrutura já não é mais um corpo.

Ex. 51 — Sorteie dois números a, b, ambos entre dois e N. Qual é a probabilidade de $a \mid b$?

Ex. 52 — Calcule $\operatorname{mdc}(294, 306)$, $\operatorname{mdc}(96, 36)$ e $\operatorname{mdc}(45, 67)$.

Ex. 53 — Determine todos os $152 \geq n \in \mathbb{N}$ tais que $\operatorname{mdc}(n, 152) = 8$. Explique seu método.

Ex. 54 — Sabendo que $b|(a-1)$, calcule $\operatorname{mdc}\left(ab\text{-}b^2, a^2\text{-}2ab + b^2 + a\text{-}b\right)$.

Ex. 55 — No enunciado do Teorema 4.4 dissemos que a e b não podem ser ambos nulos. Mostre porque a demonstração não vale para $(0, 0)$.

Ex. 56 — Prove o Teorema 4.8.

Ex. 57 — Quando apresentamos o algoritmo de Euclides, mencionamos que o valor absoluto pode ser definido facilmente em qualquer anel com relação de ordem total. Mostre uma possível definição.

Ex. 58 — Prove que $\forall x \in \mathbb{Z}, \ \operatorname{mdc}(a, b) = \operatorname{mdc}(a, xa + b)$.

Ex. 59 — Prove o Teorema 4.9.

Ex. 60 — Fazendo uso estritamente das definições dadas neste Capítulo,

(a) determine $\operatorname{mdc}(0, 0)$;

(b) já que, como dito no Exercício 41, a relação "divide" é de ordem, determine o maior e o menor elemento de $\mathbb{N}$, usando esta relação de ordem. Esboçe o diagrama de Hasse;

(c) comente a idéia de trocar a definição de $\operatorname{mdc}(a, b)$ para "o maior (usando '$\leq$') elemento que divide tanto a como b", relacionando com os itens (a) e (b) deste exercício.

[23] **Exemplo 2.19:** (Subanel do anel dado no Exemplo 2.18) O anel de matrizes da forma

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix},$$

onde $a, b \in \mathbb{Q}$ (ou $a, b \in \mathbb{R}$), com determinante não nulo é um corpo porque além de ser um anel, nele a multiplicação é comutativa; e todas as matrizes tem inversa (todas são unidade), exceto a matriz zero.

Ex. 61 — Prove o Teorema 4.5. Dica: use o Corolário 4.1.

Ex. 62 — Demos duas demonstrações do Teorema 4.4, uma delas usando o Lema de Euclides, e uma usando o Lema de Bézout. Isso imediatamente levanta uma questão: o Lema de Euclides seria consequência simples do Lema de Bézout?
(Ou – tente demonstrar o Lema de Euclides usando o Lema de Bézout)

Ex. 63 — Apresente **duas** demonstrações diferentes para o Lema 4.9.

Ex. 64 — Demonstre o Lema 4.10.

Ex. 65 — Demonstre o Teorema 4.17.

Ex. 66 — Se trocarmos os dois valores iniciais na sequência de Fibonacci, teremos uma sequência diferente (por exemplo, com o primeiro número igual a 1 e o segundo igual a 3 tem-se a *sequência de Lucas*). Ainda valem o Lema de Honsberger (Lema 4.11) e os Teoremas 4.15, 4.16? Para quais pares de valores iniciais?

Ex. 67 — (Fácil) A *fórmula de Euler-Binet*, mencionada no Teorema 4.14, é uma forma fechada para o n-ésimo número de Fibonacci. Apresentamos a fórmula novamente, mas expandindo a razão áurea:

$$\begin{aligned} u_n &= \frac{\phi^n - \hat{\phi}^n}{\sqrt{5}} \\ &= \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}. \end{aligned}$$

Seja $B(p,n)$ uma generalização da fórmula de Euler-Binet, onde o primo é parametrizável:

$$B(p,n) = \frac{(1+\sqrt{p})^n - (1-\sqrt{p})^n}{2^n\sqrt{p}}.$$

Prove que $B(p,n)$ sempre é racional.

Ex. 68 — Prove o Lema 4.12 em detalhes.

Ex. 69 — Prove o Teorema 4.19.

Ex. 70 — Prove que $\operatorname{mdc}(a+b, a\text{-}b) \geq \operatorname{mdc}(a,b)$.

Ex. 71 — Calcule $\operatorname{mmc}(22,24)$, $\operatorname{mmc}(31,34)$, $\operatorname{mmc}(20,32)$.

Ex. 72 — Prove o Teorema 4.11.

Ex. 73 — Prove o Teorema 4.12

Ex. 74 — Prove que para $k > 0$, $\operatorname{mmc}(ka,kb) = k\operatorname{mmc}(a,b)$.

Ex. 75 — Prove que $n^3 - n$ é divisível por 6 para todo inteiro n.

Ex. 76 — Prove que se $\mathrm{mmc}(a, b) = \mathrm{mdc}\,(a, b)$ então $a = \pm b$.

Ex. 77 — Prove que se $\mathrm{mdc}\,(a, b) + \mathrm{mmc}(a, b) = a + b$ então $a \mid b$ ou $b \mid a$.

Ex. 78 — Prove que $\mathrm{mdc}\,(a, 2 + a)$ sempre é 1 ou 2, para todo inteiro a.

Ex. 79 — Para quais números $\mathrm{mmc}(a, b) - \mathrm{mdc}\,(a, b) = a + b$?

Ex. 80 — Prove o Lema 4.5.

Ex. 81 — Prove que são equivalentes:

- $a \mid b$
- $\mathrm{mdc}\,(a, b) = |a|$
- $\mathrm{mmc}(a, b) = |b|$

Ex. 82 — Resolva o sistema:

$$\begin{aligned} \mathrm{mmc}(a, b) &= 360 \\ \mathrm{mdc}\,(a, b) &= 30 \end{aligned}$$

Ex. 83 — Demonstre o Teorema 4.13.

Ex. 84 — Prove que para quaisquer três inteiros a, b, c,

$$\mathrm{mdc}\,(\mathrm{mmc}(a, b), \mathrm{mmc}(a, c), \mathrm{mmc}(b, c)) = \mathrm{mmc}(\mathrm{mdc}\,(a, b), \mathrm{mdc}\,(a, c), \mathrm{mdc}\,(b, c))$$

Ex. 85 — Prove o Teorema 4.21.

Ex. 86 — Prove que para dois inteiros Gaussianos α e β, se $\alpha \mid \beta$ então $N(\alpha) \mid N(\beta)$.

Ex. 87 — Prove que um inteiro Gaussiano tem norma par se e somente se é múltiplo de $1 + i$.

Ex. 88 — Quantos inteiros Gaussianos existem com norma 13?

Ex. 89 — Dê um exemplo de par de inteiros Gaussianos que tenham mais de um MDC.

Ex. 90 — Prove que para quaisquer inteiros Gaussianos[24] α e β, se δ e γ são MDCs de α, β, então $\delta = u\gamma$, onde u é uma unidade $(\pm 1, \pm i)$.

[24] Não apenas inteiros Gaussianos. Isto vale em qualquer domínio Euclideano (prove!).

Ex. 91 — A função de valoração usada em $\mathbb{R}[x]$ poderia ser "o valor do polinômio no zero"? A ordem resultante seria parcial? Se a função de valoração puder ser esta, os MDCs calculados seriam os mesmos que usando "grau do polinômio" como função de valoração? Responda novamente para "o valor do polinômio em 1".

Ex. 92 — Prove que todo corpo é um domínio Euclideano.

Ex. 93 — Seja X um domínio Euclideano com função de valoração λ. Sejam $a, b \in X$, e suponha que d um máximo divisor comum de a e b. Prove que, se d' é algum divisor comum de a e b, então $\lambda(d') \leq \lambda(d)$; e que, se d' for *máximo* divisor comum de a e b, então $\lambda(d') = \lambda(d)$.

Ex. 94 — Considere as séries de potência

$$\sum_{n=0}^{\infty} a_0 + a_1 x + a_2 x^2 + \dots$$

Cada sequência de coeficientes $a_0, a_1, \dots$ resulta em uma série diferente. A soma de duas séries é realizada da maneira usual,

$$\left(\sum_{i=0}^{\infty} a_i x^i\right) + \left(\sum_{i=0}^{\infty} b_i x^i\right) = \left(\sum_{i=0}^{\infty} (a_i + b_i) x^i\right)$$

A multiplicação de duas séries (a_n) e (b_n)é dada pela convolução

$$\left(\sum_{i=0}^{\infty} a_i x^i\right) \cdot \left(\sum_{i=0}^{\infty} b_i x^i\right) = \left(\sum_{k=0}^{\infty} c_k x^k\right),$$

onde

$$c_k = \sum_{\substack{0<i,j<k \\ i+j=k}} a_i b_i.$$

Construa um domínio euclideano tendo essas séries como elementos. (Estas séries formam um anel, mas não um corpo!)

Ex. 95 — Prove que o Lema de Bézout vale em qualquer domínio Euclideano.

Capítulo 5

Primos

Tratamos agora de números primos e irredutibilidade. Definimos inicialmente números inteiros primos[1], e mais adiante tratamos dos análogos em domínios Euclideanos.

Definição 5.1 (número primo, números co-primos)**.** *Um número inteiro positivo é* ***primo*** *se e somente se é divisível apenas por* 1 *e por ele mesmo. Dois números* a *e* b *são co-primos se o único inteiro positivo que divide ambos é um – ou seja, se* $\mathrm{mdc}(a, b) = 1$*.* ◀

De início, podemos apreentar um Lema simples.

Lema 5.1. *Seja* n *um inteiro maior que um. O menor divisor* d *de* n*, com* $d > 1$*, é primo, e se* n *é composto,* $d \leq \sqrt{n}$*.*

Demonstração. Se $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, onde p_1 é o menor primo na fatoração de n, então o menor divisor de n é p_1, porque

[1] A definição de primo e co-primo que damos é a mesma usada nos Elementos de Euclides . (são a décima primeira e a décima segunda definições no sétimo livro):

> *11. Um número primo é um número que é medido pela unidade apenas.*
> *12. Números primos entre si são medidos somente por uma unidade como medida comum.*

No original,

> *ια' Πρῶτοι ἀριθμός ἐστιν ὁ μονάδι μόνῃ μετρούμενος.*
> *ιβ' Πρῶτοι πρὸς ἀλλήλους ἀριθμοί εἰσιν οἱ μονάδι μόνῃ μετρούμενοι χοινῷ μέτρῳ.*
> *(Prótoi arithmós estin o monádi móni metroumenos.*
> *Prótoi prós alliílous arithmoí eisin oi monádi móni metroúmenoi choinó métro.)*

Euclid. **The Elements**. [*S. l.*]: Green Lion Press, 2002. Edição bilíngue Inglês/Grego.

É evidente, no entanto, que a noção de divisibilidade – e consequentemente a de não-divisibilidade de um número por qualquer outro (primalidade) não surgiu inicialmente ou unicamente na Grécia ou Europa, e existia muito antes de Euclides. Há, por exemplo, textos védicos na Índia que descreviam métodos relacionaids a rituais onde a noção de divisibilidade era relevante.

- $p_1 \mid n$
- Qualquer outro divisor de n precisa ser maior que p_1, porque é uma potência de p_1 ou inclui outros primos maiores que p_1.

Se n é composto, então $n = p_1 M$. Claramente, M pode ser:

- Igual a p_1. Neste caso $n = p_1^2$, e $\sqrt{n} = p_1$;
- Maior que p_1, e $\sqrt{n} > p_1$. □

5.1 Fatoração Única em $\mathbb{Z}$

Esta seção trata do Teorema Fundamental da Aritmética, que afirma a existência da fatoração em primos para todos os inteiros. Este é um fato conhecido pelo menos desde a antiga Grécia, mas o enunciado da unicidade só foi proposto[2] por Gauss, no Disquisitiones, séculos depois de ter sido usado como uma afirmação "óbvia".

[2] Euclides conhecia o conceito de fatoração, mas não enunciou o teorma como o conhecemos hoje. Nas proposições 31 e 32 dos Elementos, Euclides enuncia

> *(31) Todo número composto é medido por algum número primo.*
> *(32) Todo número é primo ou é medido por algum número primo.*

O original:

> *(λα') Ἅπας σύνθεντος ἀριθμός ὑπὸ πρώτου τινὸς ἀριθμοῦ μετρεῖται.*
> *(la') (Ápas sýnthentos arithmos ypó prótou tinós arithmoú metreítai.)*
> *(lv') (Ápas arithmós ítoi prótó estin í ypó prótou tinós arithmoú metreítai.)*

Euclides não deu atenção à unicidade da fatoração.

Tradicionalmente diz-se que o Teorema foi revisto por Diofanto (que ainda não o demonstrou), e que demonstrações rigorosas surgiram a partir do trabalho de Gauss – o artigo 16 do Disquisitiones trata da unicidade da fatoração:

> *Um número composto pode ser resolvido em fatores primos de uma única maneira.*

O original:

> *Numerus compositus quicunque unico tantum modo in factores primos resolvi potest.*

No entanto, uma análise do trabalho do persa Kamāl al-Dīn al-Fārisī – كمال‌الدين فارسى – [3] mostra que ele havia enunciado o Teorema, antes de 1320, e provado a existencia da decomposição. al-Fārisī estava interessado em números amigáveis (conceito posteriormente redescoberto por Fermat e Descartes no Século XVII), e percebeu a necessidade de estabelecer fundamentos, incluindo o que hoje chamamos de Teorema Fundamental da Aritmética.
Agargün e Fletcher observam que, embora al-Fārisī tenha chegado próximo de demonstrar o Teorema como o conhecemos, ele aparentemente não tinha tanto interesse em fazê-lo (possivelmente porque suas influências não valorizavam essa possibilidade). al-Fārisī demonstrou que a decomposição existe, e propôs um método para determinar divisores a partir da decomposição. A unicidade era desneessária para seus objetivos, por isso não tratou dela.

[3] **Agargün**, Ahmet G.; **Fletcher**, Colin. al-Fārisī and the Fundamental Theorem of Arithmetic. **Historia Mathematica**, v. 21, p. 162–173, 1994.

A existência de uma demonstração anterior à de Gauss foi por muito tempo ignorada. Por exemplo, Jay Goldman expõe a história do Teorema mencionando Fermat, Legendre e outros matemáticos europeus, sem menção a al-Fārisī.

Lema 5.2. *Todo inteiro diferente de zero pode ser escrito como produto de primos e uma unidade (*$+1$ *ou* -1*).*

Damos duas demonstrações, uma usando o princípio da boa ordem, e uma por indução (forte).

Demonstração. (usando boa ordem). Começamos com os inteiros positivos apenas.

> Seja n o menor inteiro positivo que não seja primo, mas que não possa ser escrito como produto de primos (é um subconjunto de $\mathbb{N}$, e pelo princípio da boa ordem este elemento existe). Então, como n não é primo, $n = ab$, e necessariamente $0 < a, b < n$. Mas, como n é o *menor* inteiro (a boa ordem é usada aqui!) positivo que não pode ser decomposto em primos, então a e b podem. Mas se a e b podem ser decompostos em primos, $n = ab$ também pode, porque o produto das fatorações de a e de b é uma fatoração de n (ainda não provamos unicidade) – o que contradiz o que presumimos no início da demonstração.

Tendo provado para os positivos, temos os negativos. Como cada inteiro negativo $-n$ é igual a $(-1)n$, e n positivo tem fatoração em primos, terminamos a demonstração. □

Demonstração. (usando indução forte). Começamos com os inteiros positivos apenas.

> A demonstração é por indução em n.
> Base: se n é primo, ou se é ± 1, encerramos.
> Hipótese: todo $k < n$ pode ser escrito como produto de primos.
> Passo: Se n é primo, nada há a provar, portanto presumimos que $n = ab$. Como $n > 0$, temos $0 < a, b < n$. Mas como a e b são menores que n, podem ser decompostos em primos, e o produto das fatorações de a e de b é uma fatoração em primos de n.

Tendo provado para os positivos, temos os negativos. Como cada inteiro negativo $-n$ é igual a $(-1)n$, e n positivo tem fatoração em primos, terminamos a demonstração. □

Goldman, Jay R. **The Queen of Mathematics: A Historically Motivated Guide to Number Theory**. Natick, MA: A. K. Peters, 1998.

Página 5. Goldman observa, interessantemente, que a unicidade era aparentemente tida como óbvia para todos os antecessores de Gauss (que inclusive a usaram, sem enunciá-la como lema ou teorema), e por isso a demonstração não havia sido feita (e como mostrado por Agargün e Fletcher, al-Fārisī também não a produziu). Tudo indica que o primeiro a reconhecer a importância da unicidade foi, de fato, Gauss.

O Lema 5.2 apenas afirma que há alguma fatoração de inteiros em primos, mas não implica que esta seja única. Isto é garantido pelo Teorema Fundamental da Aritmética (5.1), enunciado a seguir.

Teorema 5.1 (Fundamental da Aritmética)**.** *Todo inteiro* $n \neq 0$ *pode ser escrito como produto de primos, e este produto é único, a não ser pela ordem.*

Demonstração. Que existe uma fatoração o Lema 5.2 garante. Falta mostrar que é única. Suponha, portanto, que haja mais de uma fatoração para um inteiro n. Retiramos das fatorações os elementos primos comuns às duas, e temos

$$M = p_1 p_2 \dots p_k = q_1 q_2 \dots q_r,$$

onde não há qualquer elemento comum nos dois lados. Mas pelo Lema de Euclides (Lema 4.3), como $p_1 \mid M$, teríamos $p_1 \mid q_1 q_2 \dots q_r$, e um dos q_i teria que ser igual a p_1, portanto temos uma contradição. □

Exemplo 5.1. *O inteiro* 4410 *é fatorado em*

$$4410 = (2)(3^2)(5)(7^2).$$ ◀

Definição 5.2 (ordem de p em n)**.** *Damos o nome de* ***ordem*** *de* p *em* n *ao expoente do primo* p *na fatoração de* n*, e denotamos* $\mathrm{ord}_p(n)$*.* ◀

Exemplo 5.2. *A fatoração de* 1400 *é* $2^3 5^2 7$*, portanto temos* $\mathrm{ord}_2(1400) = 3$*,* $\mathrm{ord}_5(1400) = 2$*,* $\mathrm{ord}_7(1400) = 1$*.* ◀

Para primos não constantes na fatoração de um número a ordem é zero: por exemplo, $\mathrm{ord}_3(1400) = 0$, $\mathrm{ord}_{11}(1400) = 0$, etc – o que nos permite escrever n como

$$\prod_{p \in \mathrm{PRIMOS}} p^{\mathrm{ord}_p(n)},$$

já que para todo primo q fora da fatoração de n teremos $\mathrm{ord}_q(n) = 0$ e $q^{\mathrm{ord}_q(n)} = 1$.

Lema 5.3. *Todo inteiro* n *pode ser escrito como produto de um quadrado perfeito* a^2 *e um natural livre de quadrados* b*:* $n = a^2 b$*.*

Demonstração. Sabemos que n tem fatoração em primos, $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_r}$. Para cada expoente a_i, se a_i é ímpar, reescreva $p_p^{a^i}$ como $p_i p_i^{a_i - 1}$. Agora todos os expoentes são ou pares, ou iguais a um. Por exemplo, reescrevemos $p_1^7 p_2^4 p_3^{11} p_4$ como $(p_1)(p_1^6) p_2^4 (p_3)(p_3^{10}) p_4$.
Escreva a fatoração com os expoentes pares à esquerda e os outros à direita. Renomeando os índices, temos

$$n = \left(p_1^{c_1} p_2^{c_2} \cdots p_s^{c_s}\right)\left(p_{s+1} \cdots p_t\right),$$

com c_i par. O lado esquerdo é claramente um quadrado perfeito, e o direito é livre de quadrados:

$$\begin{aligned} a^2 &= p_1^{c_1} p_2^{c_2} \cdots p_s^{c_s} \\ b &= p_{s+1} \cdots p_t. \end{aligned}$$

□

Exemplo 5.3. *A fatoração do número 396000 é*

$$396000 = 2^5\, 3^2\, 5^3\, 11,$$

que reescrevemos

$$\begin{aligned} 396000 &= (2)(2^4)\, 3^2\, (5)(5^2)\, 11 \\ &= (2^4)(3^2)(5^2)\, (2)(5)(11) \\ &= \Big[(2^2)(3)(5)\Big]^2\, (2)(5)(11) \\ &= a^2 b, \end{aligned}$$

com $a = (2^2)(3)(5) = 60$ *e* $b = (2)(5)(11) = 110$. *Para uma verificação trivial,* $a^2 b = 60^2 110 = 396000$. ◀

A discussão no Capítulo 3 deixou pendente a caracterização de quando a representação de racional no sistema posicional é finita. Essa caracterização é dada no Teorema 5.2, cuja demonstração é pedida no Exercício 97.

Teorema 5.2. *Uma fração irredutível* m/n *(com* $n > 0$*) tem expansão finita em base* b *se existe* $k \in \mathbb{N}$ *tal que* $n \mid b^k$.
Se, no entanto, não houver k *natural tal que* $n \mid b^k$*, então a expansão de* m/n *será infinita e periódica.*

Um exemplo notável de representação no sistema posicional é o do número um em base dez,

$$0,999\ldots = 1.$$

Isto não contradiz o Teorema 5.2, porque se um número tem representação infinita, não significa que não haja k tal que $n \mid b^k$ – um número pode ter mais de uma representação!

5.2 Números de Mersenne e de Fermat

Potências de qualquer número são evidentemente compostas ($a^b = a \cdot a^{b-1}$, quando $a, b > 1$), mas somando ou subtraindo um de cada potência identificamos números ($a^b + 1$, $a^b - 1$) que merecem alguma atenção.
Investigaremos brevemente estes dois casos, verificando quando cada um desses números pode ser primo, e para cada um deles demonstraremos um

teorema simples.
Primeiro, olhamos para o caso $a^b - 1$.

Teorema 5.3. *Se* $a^b - 1$ *é primo e* $b > 1$*, então* $a = 2$ *e* b *é primo.*

Demonstração. Suponha que $b > 1$ e $a^b - 1$ é primo. Então a deve necessariamente ser dois, porque Usando a identidade $(x^n - y^n) = (x - y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + xy^{n-2} + y^{n-1})$ com $x = a$, $y = 1$ e $n = b$, temos

$$a^b - 1 = (a - 1)(a^{b-1}a^{b-2} + \cdots + a + 1).$$

Como $(a - 1) \mid a^b - 1$ e $a^b - 1$ é primo, então necessariamente $a - 1 = 1$, e $a = 2$.
Agora suponha que b seja composto; $b = cd$. Então $2^{cd} = (2^c)^d$, e

$$\begin{aligned} 2^b - 1 &= (2^c)^d - 1 \\ &= (2^c - 1)\left[(2^c)^{d-1} + \cdots + 1\right], \end{aligned}$$

e $(2^c - 1)$ dividirá $2^b - 1$, que é primo – portanto b não pode ser composto. □

Os números investigados por Mersenne eram, portanto, da forma $2^p - 1$, com p primo[4].

Definição 5.3 (Números de Mersenne)**.** *Um número natural da forma* $2^p - 1$*, com* p *primo, é um* ***número de Mersenne*** *e denotado* M_p*. Quando* M_p *é primo, é chamado de* ***primo de Mersenne****.* ◀

Números de Mersenne apresentam uma interessante relação com números perfeitos[6].

Definição 5.4 (número perfeito)**.** n *é um* ***número perfeito*** *se é igual à soma de seus divisores próprios.* ◀

[4] Mersenne[5]. Mersenne começou a investigar estes números devido a conexão com números perfeitos. Em 1644, compilou uma tabela de primos da forma $2^p - 1$, mas a lista de Mersenne continha erros (listava números que Mersenne pensava serem primos, mas são compostos; também omitia alguns que são primos). A lista está em seu livro:

Mersenne, Marini. **Cogitata Physica-Mathematica**. [*S. l.*], 1644. `https://archive.org/details/fmarinimersennic00mers`.

[6] Números perfeitos foram descritos no livro sete dos Elementos, de Euclides:

> *Um número perfeito é aquele cujas partes são iguais a ele mesmo.*

No original,

> *Τέλειος ἀριθμός ἐστιν ὁ τοῖς ἑαυτοῦ μέρεσιν ἴσος ὤν.*
> *(Téleios arithmós estin o toís eaftoú méresin ísos ón.)*

Euclid. **The Elements**. [*S. l.*]: Green Lion Press, 2002. Edição bilíngue Inglês/Grego.

Exemplo 5.4. *O menor número perfeito é 6, porque* $1+2+3=6$.
O número 28 também é perfeito, porque seus divisores próprios são $1,2,4,7,14$, *e* $1+2+4+7+14=28$. ◀

Teorema 5.4. *Seja* 2^p-1 *um primo de Mersenne. Então* $(2^p-1)2^{p-1}$ *é perfeito.*

Demonstração. Seja $q=2^{p-1}$ um primo de Mersenne, e considere o número $r=q(2^{p-1})$. Separe os divisores próprios de r em dois conjuntos: as potência de dois e os outros divisores próprios:

$$\begin{aligned} A &= \{1,2,2^2,\ldots,2^{p-1}\},\\ B &= \{q,2q,2^2q,\ldots,2^{p-2}q\}. \end{aligned}$$

Ao descrever o conjunto B, excluímos o expoente $p-1$, porque queremos apenas os divisores próprios (que também são usados na definição de números perfeitos). Se tivéssemos incluído $p-1$, teríamos incluído o próprio r.
Sabemos que

$$1+x+x^2+\cdots+x^{k-1}=\frac{x^k-1}{x-1},$$

portanto a soma de A é

$$\begin{aligned} \sum_{a\in A} a &= 1+2^2+\cdots+2^{p-1}\\ &= \frac{2^p-1}{2-1}\\ &= 2^p-1\\ &= q. \end{aligned}$$

A soma de B é

$$\begin{aligned} \sum_{b\in B} &= q+2q+2^2q+\cdots+2^{p-2}q\\ &= q(1+2^2+\cdots+2^{p-2})\\ &= q\left(\frac{2^{p-1}-1}{2-1}\right)\\ &= q(2^{p-1}-1). \end{aligned}$$

Então, a soma de todos os divisores (soma de $A\cup B$) é

$$\begin{aligned} q+q(2^{p-1}-1) &= q+q(2^{p-1})-q\\ &= q(2^{p-1}), \end{aligned}$$

e r é perfeito. □

Exemplo 5.5. *Para* $p = 2, 3, 5$*, temos*

$$(2^p - 1)2^{p-1} = (2^2 - 1)2^{2-1} = 3 \cdot 2 = 6$$
$$(2^p - 1)2^{p-1} = (2^3 - 1)2^{3-1} = 7 \cdot 4 = 28$$
$$(2^p - 1)2^{p-1} = (2^5 - 1)2^{5-1} = 127 \cdot 64 = 8128$$

Já mostramos no Exemplo 5.4 que 6 *e* 28 *são perfeitos. Os divisores de* 8128 *são*

$$1, 2, 4, 8, 16, 32, 64, 127, 254, 508, 1016, 2032, 4064.$$

A soma destes é

$$1 + 2 + 4 + 8 + 16 + 32 + 64 + 127 + 254 + 508 + 1016 + 2032 + 4064 = 8128. \blacktriangleleft$$

Passamos aos números da forma $a^b + 1$.

Teorema 5.5. *Se* $a^b + 1$ *é primo, com* $a > 1$ *e* $b > 1$*, então* a *é par e* b *é potência de dois.*

Demonstração. Suponha que a é ímpar Então $a > 2$ e a^b deve ser ímpar, o que implica que $a^b + 1$ é par, e maior que dois – uma contradição, dado que é primo. Logo, a é necessariamente par.
Agora suponha que b não é potência de dois. Então $b = cq$, sendo q ímpar e $c > 0$ (um número é potência de dois se e somente se não tem fatores ímpares, por isso presumimos que b tem algum fator impar).
Usando a identidade

$$(x^n - y^n) = (x - y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + xy^{n-2} + y^{n-1})$$

com $x = a^c$, $y = -1$ e $n = q$, temos

$$(a^c)^q - (-1)^q = (a^c - (-1)^q)\left[(a^c)^{q-1} + \cdots + (-1)^{q-1}\right]$$
$$(a^c)^q - (-1)^q = (a^c + 1)\left[(a^c)^{q-1} + \cdots + (-1)^{q-1}\right] \qquad (q \text{ ímpar})$$
$$a^{cq} + 1 = (a^c + 1)\left[(a^c)^{q-1} + \cdots + (-1)^{q-1}\right] \qquad (q \text{ ímpar})$$
$$a^n + 1 = (a^c + 1)\left[(a^c)^{q-1} + \cdots + (-1)^{q-1}\right],$$

ou seja, $(a^c + 1)$ divide $a^n + 1$. Mas $a^n + 1$ é primo, e chegamos a uma contradição. Dessa forma, b não tem fatores ímpares – ou seja, é potência de dois. □

O Teorema 5.5 dá uma motivação para a definição de números de Fermat (que são da forma $2^{2^n} + 1$). Pierre de Fermat conjecturou que todos ou

números dessa forma fossem primos, mas Euler posteriormente mostrou que o quinto número de Fermat, F_5, é composto:

$$\begin{aligned} 641 &= 2^4 + 5^4 \\ &= 5 \cdot 2^7 + 1, \end{aligned}$$

portanto $2^4 = 641 - 5^4$. Agora, $F_5 = 2^{32} + 1$. e

$$\begin{aligned} 2^{32} &= 2^{28} \cdot 2^4 \\ &= 2^{28} \cdot (641 - 5^4) \\ &= 2^{28}641 - 2^{28}5^4 \\ &= 2^{28}641 - (2^7 5)^4 \\ &= 2^{28}641 - (641 - 1)^4 \\ &= 641Q - 1, \end{aligned}$$

e $641 \mid 2^{32} + 1$.

Tendo um fator, dividimos F_5 por ele e obtemos $F_5 = 2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417$ (interessantemente, o outro fator, 6700417, é primo)[7].

Definição 5.5 (Números de Fermat)**.** *Um número natural da forma $2^{2^n} + 1$, com $n \in \mathbb{N}$, é um **número de Fermat** e denotado F_n. Quando F_n é primo, é chamado de **primo de Fermat**.* ◀

Teorema 5.6. *Para $n > 0$, $F_n = F_0 \cdots F_{n-1} + 2$.*

Demonstração. Por indução em n.

Para a base, $n = 1$. Observamos que $F_0 = 3$ e $F_1 = 5$, e temos trivialmente $F_1 = F_0 + 2 = 5$.

Para o passo, presuma $F_n = F_0 \cdots F_{n-1} + 2$.

[7] Calcular 2^{32} para obter F_5 não era difícil para Fermat e Euler: basta iniciar com 1 e multiplicar repetidamente por 2. Dividir 4294967297 por 641 também não era difícil. Fatorar inteiros já não é simples, e embora $2^{32} + 1$ seja um número fácil de fatorar para computadores atuais, o problema de fatorar inteiros serviu de base para a Criptografia de chave pública por décadas (o tamanho recomendado para chave em 1974, quando o criptossistema RSA foi criado, era de 512 bits, que se traduz em inteiros da ordem de 2^{512}, mas sem computadores, fatorar um número próximo de 2^{32} certamente não é tarefa simples). Por isso é interessante Euler ter encontrado um caminho para obter esse fator, ainda que não tenha encontrado método geral de fatoração rápida.

$$\begin{aligned} F_0 \cdots F_n + 2 &= F_0 \cdots F_{n-1} F_n + 2 \\ &= (F_n - 2) \cdot F_n + 2 && \text{(hipótese de indução)} \\ &= (2^{2^n} - 1)(2^{2^n} + 1) + 2 \\ &= (2^{2^{n+1}} - 1) + 2 \\ &= F_{n+1}. && \square \end{aligned}$$

Teorema 5.7. *Se* $m \neq n$*, então* $\operatorname{mdc}(F_m, F_n) = 1$.

O enunciado faz sentido porque tratamos de "números" de Fermat (não necessariamente primos).

Demonstração. Presuma $m < n$, e seja d um divisor comum de F_m e F_n. Se $d \mid F_m$, pelo Teorema 5.6,

$$d \mid F_0 \cdots F_{n-1} + 2.$$

Note que, como $m < n$, F_m está no produto, por isso a afrimação vale. Mas se d divide F_m, então temos

$$\begin{aligned} &d \mid F_0 \cdots d \cdots F_{n-1} + 2 \\ &d \mid (F_0 \cdots F_{n-1})d + 2 \\ &d \mid 2. && \text{(subtraímos múltiplo de } d\text{)} \end{aligned}$$

Mas como todo número de Fermat é ímpar e d é divisor de F_m, d é ímpar, e portanto só pode ser um. $\square$

5.3 Infinitos primos

Antes de abordar a infinitde dos primos, definimos números primoriais, que serão usados em uma das demonstrações.

Definição 5.6 (primorial)**.** *Para* $n \in \mathbb{Z}$*, o* ***primorial*** *de* n *é o produto de todos os primos menores ou iguais a* n*. O primorial de* n *é denotado* $n\#$*.*

$$n\# = \prod_{\substack{p_i \text{ primo}, \\ p_i \leq n}} p_i. \qquad \blacktriangleleft$$

A definição implica que $0\# = 1\# = 1$, porque o produtório de nenhum número é 1 (o neutro multiplicativo). O mesmo ocorre com o fatorial.

Exemplo 5.6.

$$\begin{aligned} 3\# &= 2 \cdot 3 = 6, \\ 6\# &= 2 \cdot 3 \cdot 5 = 30, \\ 10\# &= 2 \cdot 3 \cdot 5 \cdot 7 = 210. \end{aligned}$$ ◀

Mostramos a seguir três demonstrações diferentes para a infinitude dos números primos. Há diversas outras, e a elaboração de uma delas é pedida no Exercício 116.

Teorema 5.8. *Há infinitos inteiros primos.*

Demonstração. (de Euclides) Seja $p_1, p_2, \ldots, p_n$ uma lista finita de números primos. Seja também

$$s = 1 + p_1 p_2 \ldots p_n.$$

Ou ainda,

$$s = 1 + p_n\#$$

Seja p um fator primo de s. p não pode ser nenhum dos $p_1, \ldots, p_n$, porque se fosse, p dividiria 1. Assim, existe um primo não listado. □

A demonstração de Euclides aponta somente que, a partir de um conjunto finito de primos, é possível construir um número que não divide nenhum eles, e que não pertence ao conjunto. Não é uma prova por contradição[8] – e leva a concluir que (usando o Teorema Fundamental da Aritmética) deve

[8] O que Euclides enunciou, na proposição 20 do livro 9 dos Elementos, é que

> *Há mais números primos do que qualquer quantidade de números primos que se possa propor.*

Em Grego,

> Οἱ πρῶτοι ἀριθμοὶ πλείους εἰσὶ παντὸς τοῦ προτεθέντος πλήθους πρώτων ἀριθμῶν.
> *(Oi prótoi arithmoí pleíous eisí pantós toú protethéntos plíthous próton arithmón.)*

E é exatamente o que a demonstração garante. Euclides não falava de conjuntos infinitos, por isso não provou que "existem infinitos" primos. Uma análise detalhada é dada no artigo

> **Hardy**, Michael; **Woodgold**, Catherine. Prime Simplicity. **The Mathematical Intelligencer**, v. 31, n. 4, p. 44–52, 2009.

É interessante que o que Euclides fez foi enunciar e demonstrar algo que *parece ser* um passo de indução. Usamos cuidado ao ler o enunciado, no entanto: a demonstração garante que existe algum conjunto, maior do que qualquer conjunto finito proposto. Isso nos garante que existe um conjunto infinito de primos (e nada é dito sobre este conjunto infinito ser ou não ser o conjunto de todos os primos). De fato, o primorial somado de um pode ou não ser primo. O que o enunciado garante é que $p_1, p_2, \ldots, p_n \nmid s$, mas pode haver algum p_m, fora desse conjunto, que divida s. Por exemplo,

$$13\# = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509.$$

O enunciado é válido, mas $59 > 13$ e $509 > 13$, e portanto podem dividir $13\# + 1$.

haver mais um novo primo na fatoração desse outro número (mas não podemos concluir que s é primo – somente que *tem um fator primo* que não está no conjunto!).
A demonstração de Hermite[9] tem semelhanças com a de Euclides.

Demonstração. (de Hermite) Tome um natural qualquer n. Seja p um primo divisor de $n! + 1$. Mostraremos que $p > n$ – e como isso vale para *qualquer* n, há infinitos primos (dado um $n \in \mathbb{N}$, existe primo maior que n).
Suponha, por absurdo, que $p \leq n$. Então $p \mid n!$. Mas presumimos que p é divisor de $n! + 1$. Pelo Lema 4.1, p deve dividir a diferença entre eles, $(n!+1)-(n!)$. Então $p \mid 1$ – absurdo. Portanto $p > n$, e há infinitos primos. □

Erdös[10] desenvolveu uma demonstração combinatória muito simples para o Teorema da infinitude dos primos.

Demonstração. (de Erdös, adaptada) Suponha que há um conjunto finito de primos, $p_1, p_2, \ldots, p_k$. Pelo Lema 5.3, cada número inteiro positivo n pode ser escrito como o produto de um quadrado perfeito e um não-quadrado ($n = a^2 b$). Disso seguem alguns fatos:

- Como $a \leq \sqrt{n}$, há no máximo $\sqrt{n}$ possibilidades para a
- Como b é produto de primos *distintos* (não contém quadrados na fatoração), e há k primos, então há 2^k possibilidades para b.
- Há, portanto, $2^k\sqrt{n}$ possibilidades para $a^2 b$. Como evidentemente existem n inteiros positivos entre 1 e n, então

$$\begin{aligned} n &\leq 2^k\sqrt{n} \\ n^2 &\leq (2^k)^2 n \\ n &\leq (2^k)^2. \end{aligned}$$

Assim, todo inteiro positivo n seria menor ou igual que 2^{2k}, e os naturais seriam finitos. □

Teorema 5.9. *Há distâncias arbitrariamente grandes entre primos consecutivos.*

[9] Charles Hermite (1822-1901), Francês.
[10] Paul Erdös (1913-1996), Húngaro.

Demonstração. Considere a sequência de inteiros consecutivos (com $n > 1$):

$$\begin{aligned}
&(n+1)!+2,\\
&(n+1)!+3,\\
&\quad\vdots\\
&(n+1)!+n,\\
&(n+1)!+(n+1),
\end{aligned}$$

O primeiro é divisível por 2; o segundo é divisível por 3, e assim por diante, até o último, que é divisível por $n+1$. Nenhum deles, portanto, é primo. □

A distância na demonstração é um mínimo – pode haver compostos antes de $(n+1)!+2$ e depois de $(n+1)!+(n+1)$.
Podemos ilustrar o Teorema escolhendo um número qualquer. Tomamos $n = 4$ (escolhemos um número pequeno porque teremos que calcular o fatorial de $n+1$). Assim, $n+1 = 5$, e $(n+1)! = 120$.

k	$(n+1)!+k$
2	122
3	123
4	124
5	125

Todos são compostos ($2 \mid 122, 3 \mid 123, 4 \mid 124, 5 \mid 125$). Observe que $120, 121$ (antecessores da sequencia) e 126 (sucessor) também são compostos, embora isto não fosse garantido pelo enunciado do Teorema.
Terminamos esta seção com um Teorema a respeito da série $1/p$ (soma dos recíprocos dos primos).

Teorema 5.10. *A série*

$$\sum_{p \text{ primo}} \frac{1}{p}$$

diverge.

A demonstração a seguir é de Paul Erdös.

Demonstração. Presuma que $\sum_{p \text{ primo}} \frac{1}{p} < \infty$. Nada presumimos a respeito do valor da série, mas sabemos que, como $1/p$ tende a zero (porque há infinitos primos, e há primos arbitrariamente grandes), existe uma série começando de algum primo com valor menor que $1/2$. Ou seja, existe k inteiro tal que

$$\sum_{i>k} \frac{1}{p_i} < \frac{1}{2}.$$

onde p_i é p i-ésimo primo.

Agora, para qualquer inteiro positivo x podemos definir o conjunto

$$M_x = \{n \leq x \ : \ \text{se } p > k, p_k \nmid n\}$$

dos números menores ou iguais a x, que *não* são divisíveis por primos maiores que p_k.

Se $n \in M_x$, então, como qualquer outro inteiro, n pode ser escrito como

$$n = m^2 r,$$

com r livre de quadrados.

Como $n \leq x$ e $= m^2 r$ há no máximo $\sqrt{x}$ possíveis valores para m, e 2^k possibilidades para r (porque há no máximo k primos diferentes que dividem n, e r é livre de quadrados). Assim,

$$|M_x| \leq 2^k \sqrt{x}.$$

Agora olhamos para os números que não incluímos em M_x – aqueles que são múltiplos de algum $p_r > p_k$

$$N_{i,x} = \{n \leq x \ : \ \exists j > k, p_j \mid n\}.$$

Então

$$\{1, 2, \ldots, x\} \setminus M_x = \bigcup_{i>k} N_{i,x},$$

e

$$|N_{i,x}| \leq \frac{x}{p_i}.$$

$$\begin{aligned}
x - |M_x| &\leq \sum_{i>k} |N_{i,x}| < \sum_{i>k} \frac{x}{p_i} \\
x - |M_x| &< \sum_{i>k} \frac{x}{p_i} \\
x - |M_x| &< x \sum_{i>k} \frac{1}{p_i} \\
x - |M_x| &< x \frac{1}{2} && \text{(da nossa hipótese)} \\
x &< \frac{x}{2} + |M_x| \\
\frac{x}{2} &< |M_x|.
\end{aligned}$$

Então, das duas desigualdades que obtivemos,

$$\frac{x}{2} < |M_x| \leq 2^k\sqrt{x}$$
$$\frac{x}{2} < 2^k\sqrt{x},$$

mas para $x > 2^{2k+2}$,

$$x > 2^{2k+2}\frac{x}{2} > 2^{xk+1}.$$

Como chegamos a uma contradição, concluímos que a série $\sum \frac{1}{p_i}$ diverge. □

5.4 $4k+1$, $4k+3$

O único inteiro primo par é o número dois, portanto todos os outros primos, quando divididos por quatro, devem resultar em resto um ou três. Dizemos que estes primos são *da forma* $4n+1$ ou *da forma* $4n+3$. Um dos mais antigos registros de estudos de primos dessas duas diferentes formas é de Diofanto de Alexandria[11].

Inicialmente observamos que os números (não apenas primos) da forma $4n+1$ são fechados para multiplicação:

$$(4a+1)(4b+1) = 4(4ab+a+b)+1 \tag{5.1}$$

Teorema 5.11. *Há infinitos primos da forma* $4k+3$.

[11] Diofanto estudava números inteiros que pudessem ser escritos como soma de dois quadrados. A distinção entra "$4k+1$" e "$4k+3$" está em sua "Aritmética". Diofanto escrevia "$4k-1$" ao invés de "$4k+3$", talvez (especulação nossa) porque não reconhecia o zero como número (e o primo 3, portanto era para ele "$4k-1$", com $k=1$; quando temos o zero como um número, podemos dizer que 3 é $4k+3$, com $k=0$). Nem Euclides (Século III aEC) e nem Diofanto (Século III EC) usavam o numeral zero. A primeira menção a esta separação de primos nas duas formas ocorre no item (problema) 9, do livro V do *Aritmética* (*ΑΡΙΘΜΗΤΙΚΩΝ*):

> *9. Dividir uma unidade em duas partes de maneira que, se o mesmo número for adicionado a qualquer das partes, o resultado será um quadrado. Condição necessária: o número dado não pode ser ímpar e seu dobro* $+1$ *não pode ser divisível por nenhum primo que, quando aumentado de* 1*, é divisível por* 4*.*

O problema de que Diofanto tratava neste item não nos interessa neste momento – apenas apontamos que a parte destacada é exatamente a descrição de primos da forma "$4k+3$". A tradução do Grego para o Latim,

> *Unitatem partiri in duas fractiones et addere utrique segmento datum numerum ita ut fiat quadratus. Oportet nempe datum neque imparem esse neque huius duplum plus 1 dividi per aliquem primum numerum qui, addito 1, habeat quadrantem.*

Aqui "habeat quadrantem" é, literalmente, "tem um quadrante", ou "tem um quarto" (é divisível por quatro).

Demonstração. Suponha que haja um número finito de primos da forma $4k+3$, e que estes sejam $p_1, p_2, \ldots, p_k$. Então seja

$$q = 4(p_1 p_2 \ldots p_r) - 1.$$

Este número é da forma $4k+3$ (que é a mesma coisa que $4k-1$).
Claramente, nenhum dos primos $4k+3$ divide q, Então, *todos* os fatores primos de q devem ser da forma $4k+1$. Mas pela propriedade de fechamento para multiplicação, q também deveria ser $4k+1$, o que é um absurdo. Concluímos que deve haver infinitos primos da forma $4k+3$. □

Para $4k+1$ apresentamos uma demonstração simples por redução ao absurdo, que depende do Lema 5.4, e uma família de demonstrações que depende de uma propriedade da de somas de quadrados (Lema 5.5).

Lema 5.4. *Se $n > 2$, então todo divisor ímpar de n^2+1 é da forma $4k+1$.*

A demonstração do Lema 5.4 não é dada neste momento.

Exemplo 5.7. *Seja $n = 5$. Então $n^2+1 = 26$, e os divisores de 26 são $1, 2, 13, 26$, sendo os ímpares $4(0)+1 = 1$ e $4(3)+1 = 13$.*
Para $n = 6$, temos $n^2+1 = 37$, com divisores $1, 37$, e $4(9)+1 = 37$.
Para $n = 9$, da mesma forma temos $9^2+1 = 82$, e os divisores de 82 são $1, 2, 41, 82$; Neste caso também $4(10)+1 = 41$. ◄

Teorema 5.12. *Há infinitos primos da forma $4k+1$.*

Demonstração. (usando o Lema 5.4) Suponha que o número de primos da forma $4n+1$ seja finito, e que estes sejam $p_1, p_2, \ldots, p_k$. Construa agora o número

$$r = 4p_1^2 p_2^2 \ldots p_k^2 + 1.$$

Nenhum dos p_i pode dividir r. Então os divisores primos de r não estão entre os $p_1, \ldots, p_k$ usados para construir r – devem então ser da forma $4k+3$. Mas como r é da forma x^2+1, pelo Lema 5.4[12], r não pode ser divisível por um ímpar da forma $4k+3$. Chegamos a uma contradição, e a demonstração está finalizada. □

A demonstração dada é por contradição, e seria interessante se houvesse outra, construtiva, de onde pudéssemos extrair um método para construir primos da forma $4k+1$.
Há uma demonstração construtiva pra o Teorema 5.12, publicada em 1992 por Neville Robbins[13]. Esta demonstração, no entanto, depende do Lema 5.5, que apresentamos por ora sem demonstração (que será dada no Capítulo 10).

[12] **Lema 5.4:** Se $n > 2$, então todo divisor ímpar de n^2+1 é da forma $4k+1$.
[13] Neville Robbins (1938–), Belga-Americano.

Lema 5.5. *Se n é soma de dois quadrados, $n = a^2 + b^2$, com $\mathrm{mdc}(a, b) = 1$, então n não tem fatores primos da forma $4k + 3$.*

No Lema 5.5, "não haver fatores primos da forma $4k + 3$" significa efetivamente que não há divisores (primos ou não) da forma $4k + 3$.
Embora Robbins tenha redigido a demonstração sem dividí-la em partes, neste texto apresentaremos a essência dela em um Lema, e depois a completaremos de duas formas diferentes, uma usando números de Fermat, e uma usando números de Fibonacci (as duas variantes foram originalmente apresentadas na mesma demonstração por Robbins). Nossa apresentação é ligeiramente diferente da original.

Lema 5.6. *Seja (s_n) uma sequência com as seguintes propriedades:*

i) $s_n > 1$ *quando* $n \geq 1$*;*

ii) $s_n = a_n^2 + b_n^2$*, com* $\mathrm{mdc}(a, b) = 1$*;*

iii) $\mathrm{mdc}(s_n, s_m) = 1$ *quando* $n \neq m$*;*

iv) a_n *e* b_n *tem paridades diferentes (um é par e o outro é ímpar).*

Então cada s_n tem um fator primo da forma $4k+1$, que não está na fatoração dos outros elementos s_j da sequência.

Demonstração. A sequência s_n tem as seguintes propriedades:

i) $s_n > 1$ quando $n \geq 1$ (por definição).

ii) Para todo n, existe algum primo $p = 4k+1$ tal que $p \mid s_n$ (pelo Lema 5.5, não há divisores $4k + 3$, e pela condição (iv) do enunciado, não há divisores $4k$ nem $4k + 2$).

iii) Todos os s_n são co-primos entre si.

A exclusão de divisores $4k$ e $4k + 2$ é relevante para excluir sequências de potências de dois. Por exemplo, a sequência $d_n = 2^n$, que contém somas de quadrados $d_i = (2^{i-2})^2 + 0^2$, satisfaria os critérios, mas seus elementos não contém primos $4k + 1$. O único primo nas fatorações desses números é o 2.
Claramente, cada s_n nos dá um novo primo da forma $4k+1$, porque todos os elementos tem um divisor da forma $4k + 1$, que é diferente para cada novo elemento da sequência, porque são todos co-primos. □

A seguir serão detalhadas duas demonstrações para o Teorema 5.12 (infinitude dos primos $4K + 1$). Ambas constróem a sequência $s_n = a_n^2 + b_n^2$, com $\mathrm{mdc}(a, b) = 1$ e a e b tendo paridades diferentes. A demonstração usando números de Fibonacci, também usamos o Lema 5.7 (Exercício 106).

Lema 5.7. *Seja* p *primo. Então*

$$\mathrm{mdc}\left(\frac{p+1}{2}, \frac{p\text{-}1}{2}\right) = 1.$$

Repetimos agora o enunciado do Teorema 5.12, e passamos às duas demonstrações.
Teorema 5.12: Há infinitos primos da forma $4k+1$.

Demonstração. (usando números de Fermat)
Considere a sequência (F_n), de números de Fermat (não necessariamente primos).

i) $F_n > 1$;

ii) F_n é evidentemente soma de quadrados: $F_n = 2^{2n}+1 = (2^{2n-1})^2+(1)^2$, $\mathrm{mdc}\left(2^{2n\text{-}1}, 1\right) = 1$, e obviamente as paridades de 2^{2n-1} e 1 são opostas.

iii) Todos os F_n são co-primos entre si (Teorema 5.7).

Basta agora usar o Lema 5.6. □

Também é possível usar números de Fibonacci, embora a demonstração fique um pouco mais longa.

Demonstração. (usando números de Fibonacci)
Considere a sequência (u_n), de números de Fibonacci (não necessariamente primos). Observamos os fatos a seguir.

I) $u_{2n+1} = u_n^2 + u_{n+1}^2$ (Teorema 4.17);

II) $\mathrm{mdc}\,(u_m, u_n) = u_{\mathrm{mdc}(m,n)}$ (Teorema 4.16);

III) $2 \mid u_n$ se e somente se $3 \mid n$ (Teorema 4.18);

IV) $u_n > 1$ quando $n > 2$.

Enumere agora os primos maiores que 3: $q_1 = 5$, $q_2 = 7$, etc. Defina uma sequência (s_n), de forma que o n-ésimo termo de s_n seja o número de Fibonacci com índice q_n:

$$s_n = u_{q_n}.$$

Observamos que, por (I),

$$u_{q_n} = u^2_{\left[\frac{q_n-1}{2}\right]} + u^2_{\left[\frac{q_n+1}{2}\right]}. \tag{5.2}$$

Agora, embora os q_i sejam primos, precisamos garantir que os dois números elevados ao quadrado em 5.2 são co-primos.

Como pelo Lema 5.7 $\mathrm{mdc}\,((q_n\text{-}1)/2, (q_n+1)/2)) = 1$, então por (II),

$$\mathrm{mdc}\left(u_{\left[\frac{q_n\text{-}1}{2}\right]},\ u_{\left[\frac{q_n+1}{2}\right]}\right) = 1. \tag{5.3}$$

Como $q_n > 3$, e q_n é primo, (III) implica que $2 \nmid u_{q_n}$, portanto se considerarmos

$$u_{\left[\frac{q-1}{2}\right]}, \qquad u_{\left[\frac{q+1}{2}\right]}, \tag{5.4}$$

um é par e o outro, ímpar.
Finalmente, quando $m \neq n$, $q_m \neq q_n$, então $\mathrm{mdc}\,(q_m, q_n) = 1$. Por isso, a partir de (II) concluímos que $\mathrm{mdc}\,(u_{q_m}, u_{q_n}) = 1$. Temos:

i) $q_n > 1$ (de (IV));

ii) $q_{2n+1} = q^2_{\frac{n-1}{2}} + q^2_{\frac{n+1}{2}}$, com os dois elementos elevados ao quadrado sendo co-primos (Equação 5.3) e com paridade diferentes (Equação 5.4);

iii) $\mathrm{mdc}\,(u_{q_m}, u_{q_n}) = 1$, porque os q_i são co-primos, e $\mathrm{mdc}\,(u_m, u_n) = u_{\mathrm{mdc}(m,n)}$ (Teorema 4.16[14]).

Pelo Lema 5.6, a sequência (q_n) nos dá infinitos primos da forma $4k+1$. □

5.5 Fatoração Única em Dominios Euclideanos

Lembramos que em um anel, as *unidades* são os elementos com inversos. Em $\mathbb{Z}$, estes são ± 1; em $\mathbb{R}[x]$, são os polinômios constantes (os de grau zero), porque para outros polinômios, $1/p$ não é polinômio; nos inteiros Gaussianos ($\mathbb{Z}[i]$), as unidades são ± 1 e $\pm i$.

Definição 5.7 (elemento irredutível)**.** *Um elemento x é **irredutível** se é divisível somente por unidades ou por seus próprios múltiplos por unidade (ux, onde u é unidade).* ◄

Assim, um polinômio não constante p é irredutível se os únicos outros polinômios que dividem p são constantes ou múltiplos de p. Por exemplo, o polinômio $x^2 + x$ não é irredutível, porque

$$x^2 + x = x(x+1)$$

e portanto $x \mid x^2 + x$, e $(x+1) \mid x^2 + x$.

[14] **Teorema 4.16:** $\mathrm{mdc}\,(u_m, u_n) = u_{\mathrm{mdc}(m,n)}$.

Já x^2+1 é irredutível em $\mathbb{R}[x]$, no anel de polinômios com coeficientes reais, porque seus divisores são somente os polinômios constantes e os múltiplos deste mesmo polinômio.
A redutibilidade de um polinômio depende do anel onde trabalhamos. Podemos deixar de lado o anel dos polinômios com coeficientes reais e passar para o anel dos polinômios com coeficientes inteiros[15]. Um polinômio que é fatorável em $\mathbb{R}[x]$ pode ser irredutível em $\mathbb{Z}[x]$. Por exemplo, o polinômio x^2+x-1 tem duas raízes racionais, logo é fatorável na forma $(x-r_1)(x-r_2)$:

$$x^2+x-1=\left(x-\frac{\sqrt{5}-1}{2}\right)\left(x+\frac{\sqrt{5}-1}{2}\right).$$

Esta fatoração implica que o polinômio é redutível em $\mathbb{R}[x]$, (polinômios com coeficientes reais) mas é irredutível em $\mathbb{Q}[x]$ (polinômios com coeficientes racionais) (porque não é produto de polinômios com coeficientes racionais) e também no anel $\mathbb{Z}[x]$, porque não é produto de outros polinômios *com coeficientes inteiros*.
Os inteiros Gaussianos irredutíveis são, da mesma forma, os divisíveis por unidades e por seus associados (múltiplos de si mesmo por unidade). Por exemplo, $1+i$ é irredutível, porque seus divisores são somente as unidades e $(\pm1)(1+i)$, $(\pm i)(1+i)$. Já $3-i$ não é irredutível, porque

$$(1-i)(2+i)=3-i.$$

A seguir iniciamos com uma demonstração, para $\mathbb{R}[x]$, de que todos elementos podem ser escritos como produto de irredutíveis; em seguida generalizamos o enunciado para domínios Euclideanos.

Lema 5.8. *Todo polinômio diferente de zero pode ser escrito como produto de polinômios irredutíveis.*

A demonstração é a mesma que fizemos, por indução, para a existência de fatoração para inteiros – apenas adaptada para polinômios.

Demonstração. Por indução no grau dos polinômios. A base se dá com $n=1$: todo polinômio de grau um é claramente irredutível. Agora presuma que todo polinômio de grau menor que n é fatorável em irredutíveis. Considere um polinômio qualquer p de grau n. Se p é irredutível, não há mais o que mostrar. Se p não é irredutível, então $p=qr$, onde os graus de q e r são menores que n. Mas então há uma fatoração para q e uma para r, e conseguimos portanto uma fatoração para $p=qr$. □

Para inteiros Gaussianos, pode-se repetir a demonstração por indução na norma. No entanto, podemos fazer melhor: uma demonstração que valha para qualquer domínio Euclideano.

[15] Verifique que de fato, ambos são anéis, e que um é subanel do outro.

Lema 5.9. *Em um domínio Euclideano,* $\lambda(u) = 1$ *se e somente se* u *é unidade.*

O Teorema Fundamental da Aritmética vale em qualquer *domínio de fatoração única*, que não definiremos. Nos basta apenas que *todo domínio Euclideano é um domínio de fatoração única*, e portanto vale o Teorema, que enunciamos novamente, ligeiramente modificado.

Teorema 5.13 (Fundamental da Aritmética em Domínios Euclideanos)**.** *Em um Domínio Euclideano* R*, todo elemento irredutível pode ser decomposto em um produto de irredutíveis e por uma unidade.*

Demonstração. Por indução em $\lambda(x)$.
Caso base: para unidades não há o que demonstrar. Para $\lambda(x) = 2$, suponha que x seja da forma

$$x = u_1 u_2 \dots u_k(t),$$

onde u_i são unidades – e portanto $\lambda(u) = 1$. Como $\lambda(x) = 2$, e t não é unidade, vemos que t não pode ser mais fatorado (não há dois inteiros cujo produto seja dois), então t é irredutível, e é sua própria fatoração.
A hipótese é que todo elemento com norma menor que n seja fatorável em irredutíveis.
Passo: seja x com norma n. Se x é irredutível, ele é sua própria fatoração. Senão, $x = ab$, e as normas de a e b são necessariamente menores que a de x. Mas neste caso, a e b tem fatorações em irredutíveis, e a fatoração de x é a multiplicação das de a e b. □

Em qualquer domínio Euclideano, elementos podem ser fatorados em irredutíveis (O Exercício 131 pede a demonstração da unicidade). A função λ usada na demonstração é, para polinômios, o grau subtraído de um[16]; para inteiros Gaussianos, a norma.
A noção de conteúdo de polinômio e o Lema de Gauss, a seguir, também valem para domínios de fatoração única; da mesma forma que fizemos com o Teorema Fundamental da Aritmética, refaremos os enunciados para Domínios Euclideanos.

Definição 5.8 (conteúdo de polinômio; polinômio primitivo)**.** *O* ***conteúdo*** *de um polinômio* p *com coeficientes em um domínio Euclideano é o MDC de seus coeficientes, denotado* $c(p)$*. Se* $c(p) = 1$*, o polinômio é* ***primitivo****.* ◀

Exemplo 5.8. *Seja* $p(x) = 6x^4 + 2x^3 + 4x$*, com coeficientes em* $\mathbb{Z}$ *(que é domínio Euclideano). O conteúdo do polinômio é* $\operatorname{mdc}(6, 2, 4) = 2$*.*
Os inteiros Gaussianos são, também, um domínio Euclideano. Os coeficientes do polinômio $(2 + i)x^2 - 3x$ *são inteiros Gaussianos, e o polinômio é primitivo, porque seu conteúdo é* $\operatorname{mdc}(2 + i, 3) = 1$*. Já o polinômio*

[16] Por que?

$(5i-1)x^3+(4+2i)x$ *tem conteúdo* $\operatorname{mdc}(5i, 4+2i) = \{2+i, -2-i, -1+2i, 1-2i\}$ *– não é, portanto, primitivo.* ◀

Lema 5.10 (de Gauss)**.** *Sejam* f, g *são polinômios com coeficientes em um domínio Euclideano, nenhum deles nulo. Então* $c(fg) = c(g)\,c(f)$*. Assim, se* f *e* g *são primitivos, então* fg *também é.*

Demonstração. O Teorema afirma que a função c é multiplicativa, e depois determina que a multiplicação de primitivos resulta em polinômio primitivo; na demonstração faremos o caminho oposto, começando pela segunda parte do enunciado.
Sejam $f(x) = a_0 + a_1x + \cdots + a_mx^m$ e $g(x) = b_0 + b_1x + \ldots + b_nx^n$ dois polinômios primitivos. Seja $k = c(fg)$. Suponha que exista um primo p que divida k. Como f e g são primitivos, existe algum coeficiente a_i de f e algum b_j de g que p não divide. Mas então existe um coeficiente a_ib_j no polinômio fg, que p não pode dividir, e portanto não existe tal primo p. Assim, fg também é primitivo.
Abordamos agora a primeira parte do enunciado. Sejam dois polinômios, não necessariamente primitivos, e e h. Sejam E e H polinômios primitivos tais que

$$\begin{aligned} e &= c(e)E \\ h &= c(h)H. \end{aligned}$$

Então

$$\begin{aligned} c(eh) &= c(c(e)\,c(h)EH) \\ &= c(e)\,c(h)\,c(EH) \\ &= c(e)\,c(h), \end{aligned}$$

porque E e H são primitivos, portanto EH é primitivo e $c(EH) = 1$. □

Exercícios

Ex. 96 — Determine todos os primos da forma $n^3 - 1$.

Ex. 97 — Demonstre o Teorema 5.2.

Ex. 98 — Mostre que se $n^2 + 2$ é primo, então $3 \mid n$.

Ex. 99 — Prove que todo primo da forma $3n + 1$ também é da forma $6k + 1$.

Ex. 100 — Prove que para todo inteiro positivo $n > 2$, existe um primo p tal que

$$n < p < n!$$

Ex. 101 — Quais são os primos p tais que $p \mid 2^p + 1$? E, generalizando, os que dividem $2^p + k$, onde k é o antecessor de um primo?

Ex. 102 — Seja p um primo ímpar, e k algum inteiro tal que $1 \leq k < p$. Prove que

$$p \left| \binom{p}{k} \right. .$$

Ex. 103 — Prove que se k e n são inteiros positivos e $\sqrt[k]{n}$ é racional, então $\sqrt[k]{n}$ é inteiro.

Ex. 104 — Suponha que $ab = c^n$, e que $\operatorname{mdc}(a, b) = 1$. Prove que existem d, e inteiros tais que

$$a = d^n, \quad b = e^n.$$

Ex. 105 — Prove que a soma de dois primos consecutivos nunca é o dobro de um primo.

Ex. 106 — Demonstre o Lema 5.7.

Ex. 107 — Prove que todo número de Fermat F_n com $n > 1$ tem o último dígito igual a 7.

Ex. 108 — Prove que nenhum número de Fermat é quadrado perfeito.

Ex. 109 — Prove que para $n > 1$, $F_n = F_{n-1} + 2^{2^{n-1}} \cdot F_0 \cdot F_1 \cdots F_{n-2}$.

Ex. 110 — Use o Teorema 5.7 para provar que há infinitos primos.

Ex. 111 — Prove que o 3 é o único natural que é número de Fermat e também é número de Mersenne.

Ex. 112 — Mostre que todo inteiro positivo pode ser escrito como soma de números de Fibonacci.

Ex. 113 — Mostre que

$$\operatorname{mdc}\left(n^{2^r} + 1,\, n^{2^s} + 1\right)$$

é sempre igual a 1 (para n par) ou 2 (para n ímpar).

Ex. 114 — Refaça a demonstração de infinitude dos primos de Euclides, mas subtraindo um ao invés de somar.

Ex. 115 — (Infinitos primos - demonstração de Stieltjes) Complete a demonstração a seguir para a infinitude dos primos: Sejam $p_1, \ldots, p_k$ todos os

primos. Seja $A = p_1 p_2 \dots p_k$, e seja $A = st$ uma fatoração de A com $s, t \geq 1$. Cada primo p_i divide s ou t, ...

Ex. 116 — (Demonstração de Euler, modernizada, para a infinitude dos primos)

i) Mostre que

$$\sum_n \frac{1}{n} = \prod_{p \text{ primo}} \frac{1}{1 - \frac{1}{p}}$$

ii) Argumente que se houvesse uma quantidade finita de primos, o lado direito seria finito, e consequentemente o lado esquerdo também.

iii) Conclua que isto é impossível, observando que a série harmônica diverge.

Ex. 117 — A soma dos dígitos de um quadrado pode ser 2451?

Ex. 118 — Prove que p é primo **se e somente se** no Triângulo de Pascal[18] a p-ésima linha é composta de números divisíveis por p, exceto pelos dois uns nas extremidades. (A primeira linha, contendo somente o número um, tem índice zero).

	1							
	1	1						
$2^a \rightarrow$	1	2	1					
$3^a \rightarrow$	1	3	3	1				
	1	4	6	4	1			
$5^a \rightarrow$	1	5	10	10	5	1		
	1	6	15	20	15	6	1	
$7^a \rightarrow$	1	7	21	35	35	21	7	1

(Note que a linha 2, $(1, 2, 1)$, contém somente o dois, que é ele mesmo divisível por dois; a linha 3 contém duas vezes o 3, divisível por 3; a linha 5, $(1, 5, 10, 10, 5, 1)$, contém múltiplos de 5; a linha sete também – contém múltiplos de sete.)

Ex. 119 — Prove o Teorema de Lucas[19] (Édouard Lucas foi o primeiro a enunciar este teorema.): Seja p primo, e m, n inteiros positivos, cuja representação **na base** p é

$$m = m_k m_{k-1} \cdots m_1 m_0$$
$$n = n_k n_{k-1} \cdots n_1 n_0$$

[18] Ver nota de rodapé 21 na página 10.
[19] Édouard Lucas (1842-1891), Francês.

Então

$$\binom{m}{n} \equiv \prod_{j=1}^{k} \binom{m_j}{n_j} \pmod{p}.$$

Mostre como este Teorema poderia ter sido usado para resolver o Exercício 118.

Ex. 120 — A respeito do Teorema de Lucas (Exercício 119): explique detalhadamente porque, apesar de estarmos usando um sistema posicional, em que os dígitos tem significados diferentes dependendo de sua posição na representação, a ordem deles não é relevante no enunciado (simplesmente toma-se o produtório sobre todos os dígitos!)

Ex. 121 — Prove que todo inteiro positivo pode ser representado como produto de um número ímpar e uma potência de dois (mesmo que seja 2^0).

Ex. 122 — Seja $p > 5$ primo. Mostre que $p - 4 \neq n^4$, com $n \in \mathbb{Z}$.

Ex. 123 — Determine com quantos zeros termina o número 100!

Ex. 124 — Para quantos n o coeficiente binomial $\binom{100}{n}$ é ímpar?

Ex. 125 — Quantas divisões sucessivas por 1344 podemos fazer com o número 50! ?

Ex. 126 — Mostre que há infinitos primos da forma $6n + 5$.

Ex. 127 — Prove o Lema 5.9.

Ex. 128 — Sejam $m = p_1^{a_1} p_s^{a_2} \cdots p_k^{a_k}$ e $n = p_1^{b_1} p_s^{b_2} \cdots p_k^{b_2}$, onde $p_1, \ldots, p_k$ são primos distintos.

a) Mostre que $\operatorname{mdc}(m, n) = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$, onde $c_i = \min(a_i, b_i)$.

b) Calcule $\operatorname{mdc}\left(2^3 7^9 17,\ 2^2 3^1 117^2\right)$.

Ex. 129 — Calcule a soma de todas as frações tais que o denominador e o numerador são (i) co-primos, e (ii) divisores positivos de 49000.

Ex. 130 — Qual é a probabilidade de dois inteiros serem coprimos?

Ex. 131 — O Teorema 5.13 afirma que em domínios Euclideanos todo elemento pode ser fatorado em irredutíveis, mas não afirma que a fatoração é única. Prove que em todo domínio Euclideano, a fatoração é única a não ser por ordem e por multiplicação por unidades. Para isto, use a Definição e o Lema a seguir.

Definição 5.9 (primo em domínio Euclideano)**.** *Em um domínio Euclideano, um elemento* p *é* ***primo*** *se e somente se vale para ele o Lema de Euclides*

(Lema 4.3, $p \mid ab$ *implica que* $p \mid a$ *ou* $p \mid b$*).* ◀

Lema 5.11. *Em um domínio Euclideano, todo elemento primo é irredutível.*

Ex. 132 — Prove o Lema apresentado no Exercício 131.

Capítulo 6

Congruências

Iniciamos o estudo de congruências, que facilitam a expressão de fatos a respeito de divisibilidade[1].

6.1 Relações de congruênca e aritmética modular

Quando tratamos de números primos, dividimos os primos ímpares entre os da forma $4k + 1$ e os da forma $4k + 3$, que é o mesmo que dizer "os que deixam resto 1 quando divididos por 4 e os que deixam resto 3 quando divididos por 4". Números que deixam o mesmo resto quando divididos por um mesmo número m tem muito em comum, e os separaremos em classes de equivalência.

[1] O tratamento moderno de congruências foi sistematizado por Gauss no *Disquisitiones Arithmeticae*.

Gauss, Johann Carl Friedrich. **Disquisitiones Arithmeticae**. [*S. l.*], 1801.

E definir congruência é a primeira coisa que faz no texto, na Seção I, "Números Congruentes em Geral". Artigo 1.
O conceito, no entanto, existiu por séculos antes disso. Maarten Bullynck oferece uma visão bastante extensa do assunto.

Bullynck, Maarten. Modular arithmetic before C.F. Gauss: Systematizations and discussions on remainder problems in 18th-century Germany. **Historia Mathematica**, v. 36, p. 48–72, 2009.

Bullyink comenta que métodos para aritmética com restos são conhecidos há muito tempo, mas foi Bachet, em 1624 (ou 1612, se considerarmos a primeira edição de seu livro) quem observou a conexão destes métodos com o algoritmo de Euclides para divisão. Também reporta que métodos para resolver problemas deste tipo eram conhecidos na China e Índia, tres ou quatro séculos a.C.

Se a e b deixam o mesmo resto quando divididos por m, então

$$\begin{aligned} a &= sm + r, \\ b &= tm + r. \end{aligned}$$

Ao subtrairmos $a - b$, teremos

$$\begin{aligned} a - b &= sm + r - tm - r \\ &= sm - tm \\ &= (s - t)m, \end{aligned}$$

portanto m divide $a - b$. Podemos, portanto, dizer que as duas afirmações são equivalentes:

i) a e b deixam o mesmo resto quando divididos por m;

ii) $m \mid a - b$.

A definição moderna de congruência, a seguir, não é diferente daquela dada por Gauss[2]

Definição 6.1 (congruência)**.** *Se $m \mid (a-b)$, ou seja, se $(a-b)/m$ é inteiro, dizemos que a é **congruente** a b módulo m, e denotamos*[3] $a \equiv b \pmod{m}$. ◀

[2] O *Disquisitiones* inicia exatamente com esta definição:

> *Se um número a divide a diferença dos números b e c, b e c são ditos congruentes relativos a a; senão, b e c são incongruentes. O número a é chamado de módulo.*
>
> *Si numerus a numerorum b, c differentiam metitur. b et c secundum a congrui dicuntur, sin minus, incongrui: ipsum a modulum appellamus.*

Somente um pouco adiante, na mesma página, o símbolo $\equiv$ é introduzido:

> *Devemos designar congruência pelo símbolo ,≡, juntando a ele entre parênteses o módulo quando for necessário; por exemplo, $-7 \equiv 15 \pmod{11}, -16 \equiv 9 \pmod{5}$.*
>
> *Numerorum congruentiam hoc signo, $\equiv$, in posterum denotabimus, modulum ubi opus erit in calusulis adiungentes, $-16 \equiv 9 \pmod{5}$. $-7 \equiv 15 \pmod{11}$.*

Gauss observa, em nota de rodapé, que

> *Adotamos este símbolo por causa da analogia entre igualdade e congruência. Pelo mesmo motivo, Legendre, no tratado que frequentemente deveremos citar, usou o mesmo símbolo para igualdade e congruência. Para evitar ambiguidade nós fizemos uma distinção.*
>
> *Hoc signum propter magnam analogiam quae inter aequalitatem atque congruentiam invenitur adoptavimus. Ob eandem caussam ill. Le Gendre in comment. infra saepius laudana ipsum aequalitis signum pro congruentia retinuit, quod nos ne ambiguitas oriatur imitari dubitavimus.*

[3] Não é a única notação que existe para congruência. Há autores que usam $a \underset{m}{\equiv} b$ para dizer que a é congruente a b módulo m.

Usualmente trataremos somente de módulos positivos, sem qualquer prejuízo, já que $m \mid (a - b)$ e $-m \mid (a - b)$ são equivalentes.

Exemplo 6.1. $30 \equiv 16 \pmod 7$, *porque* $30 - 16 = 14$, *e* $7 \mid 14$.
Também $12 \equiv 28 \pmod 8$, *porque* $12 - 28 = -16$, *e* $8 \mid -16$. ◀

Exemplo 6.2. *Se* $n \equiv 0 \pmod 2$, *então* n *é par; se* $n \equiv 1 \pmod 2$, *é ímpar; e de maneira geral,* $n \equiv 0 \pmod k$ *é uma forma de expressar que* n *é divisível por* k. ◀

Exemplo 6.3. *Os números primos ímpares podem ser de duas formas:* $p \equiv 1 \pmod 4$ *(os da forma* $4k + 1$*), e* $p \equiv 3 \pmod 4$ *(os da forma* $4k + 3$*).* ◀

Teorema 6.1. *Para todo* $m > 1$, *a relação de congruência módulo* m *é de equivalência.*

Os vários números são congruentes a k módulo m formam uma classe de equivalência. O Teorema a seguir nos possibilitará realizar operações aritméticas com as classes de congruência sem dificuldade.

Teorema 6.2. *É possível somar e multiplicar as classes de equivalência: se* $a \equiv b \pmod m$ *e* $c \equiv d \pmod m$, *então*

i) $a + c \equiv b + d \pmod m$,

ii) $ac \equiv bd \pmod m$.

Demonstração. A demonstração é direta.
(i) Pela definição de congruência, $m \mid (b - a)$ e $m \mid (d - c)$, então $m \mid (b - a) + (d - c)$, logo $m \mid (b + d) - (a + c)$, e $a + c \equiv b + d \pmod m$.
(ii) Queremos mostrar que $m \mid (bd - ac)$. Mas $bd - ac = d(b - a) + a(d - c)$, e como m divide os dois fatores em parênteses, $(b - a)$ e $(d - c)$, m divide $d(b - a) + a(d - c)$. □

Este Teorema implica também que se $a \equiv b \pmod m$, então $a^n \equiv b^n \pmod m$. Também é relevante que as classes de equivalencia de inteiros módulo n formam um anel.

Teorema 6.3. *Sejam* $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$ *as classes de equivalência módulo* n. *Damos o nome de* $\mathbb{Z}_n$, *ou* $\mathbb{Z}/n\mathbb{Z}$ *a este conjunto, que com as operações de soma e multiplicação descritas no Teorema 6.2, formam um anel comutativo com unidade.*

Havendo soma e multiplicação, é possível computar o valor de polinômios.

Teorema 6.4. *Se* p *é um polinômio com coeficientes inteiros, e* $a \equiv b \pmod m$, *então* $p(a) \equiv p(b) \pmod m$.

Demonstração. Seja $p(x) = k_n x^n + k_{n-1} x^{n-1} + \cdots + k_1 x + k_0$, e suponha $a \equiv b \pmod{m}$. Então

$$\begin{aligned} p(a) &= k_n a^n + k_{n-1} a^{n-1} + \cdots + k_1 a + k_0 \\ &\equiv k_n b^n + k_{n-1} b^{n-1} + \cdots + k_1 b + k_0 \pmod{m}, \end{aligned}$$

pelo Teorema 6.2. □

Exemplo 6.4. *Sabemos que* $17 \equiv 32 \equiv 2 \pmod{15}$*, e escolhemos um polinômio,* $p(x) = x^2 - 3x + 2$*. Então*

$$\begin{aligned} p(32) = 32^2 - 3(32) + 2 = 930 &\equiv 0 \pmod{15} \\ p(17) = 17^2 - 3(17) + 2 = 240 &\equiv 0 \pmod{15} \\ p(2) = 2^2 - 3(2) + 2 = 0 &\equiv 0 \pmod{15} \end{aligned}$$

Da mesma forma, temos $8 \equiv 19 \equiv 41 \pmod{11}$*. Escolhemos o polinômio* $q(x) = x^2 - 2x$*. Então*

$$\begin{aligned} q(3) = 8^2 - 4(8) = 32 &\equiv 10 \pmod{11} \\ q(19) = 19^2 - 4(19) = 285 &\equiv 10 \pmod{11} \\ q(41) = 41^2 - 4(41) = 1517 &\equiv 10 \pmod{11}. \end{aligned}$$

◀

Teorema 6.5. *Para todos* $a, b, c, d \in \mathbb{Z}$ *e* $1 < m \in \mathbb{Z}$*,*

(i) *se* $a \equiv b \pmod{m}$*, então* $ac \equiv bc \pmod{mc}$*;*

(ii) *se* $a \equiv b \pmod{m}$*, e* $d \mid m$*, então* $a \equiv b \pmod{d}$*.*

A lei do cancelamento para multiplicação em congruências (recíproca do item (i) do Teorema 6.5) é diferente da que vale para inteiros. Se $ab \equiv ac \pmod{m}$, não é imediato que se pode dizer que $b \equiv c \pmod{m}$.
Por exemplo, sejam $a = 15$ $b = 10$, $c = 2$ e $m = 10$. Temos

$$\begin{aligned} ab &\equiv ac \pmod{10} \\ (15)(10) &\equiv (15)(2) \pmod{10} \\ 150 &\equiv 30 \pmod{10}. \end{aligned} \qquad \text{(ok!)}$$

No entanto, não podemos cancelar o fator a nos dois lados da congruência:

$$\begin{aligned} ab &\equiv ac \pmod{10} \\ b &\equiv c \pmod{10} \\ 10 &\equiv 2 \pmod{10}. \end{aligned} \qquad \text{(não!)}$$

O Teorema 6.6 determina exatamente em que condições o cancleamento pode ser feito em multiplicações de congruências.

Teorema 6.6 (lei de cancelamento)**.** *Em congruências, o cancelamento de fatores se dá de acordo com a seguinte regra:*

$$ab \equiv ac \pmod{m} \text{ se e somente se } b \equiv c \pmod{\frac{m}{\operatorname{mdc}(a,m)}}.$$

Como caso particular,

$$\text{se } ab \equiv ac \pmod{m}. \text{ e } \operatorname{mdc}(a,m) = 1 \text{ então } b \equiv c \pmod{m}.$$

Demonstração. Mostramos primeiro que $ab \equiv ac \pmod{m}$ implica em $b \equiv c \pmod{\frac{m}{\operatorname{mdc}(a,m)}}$.

$$\begin{aligned} ab &\equiv ac \pmod{m} \\ ab - ac &= km \\ a(b-c) &= km \\ \frac{a}{\operatorname{mdc}(a,m)}(b-c) &= k\frac{m}{\operatorname{mdc}(a,m)} \\ b - c &= k\left(\frac{m}{\operatorname{mdc}(a,m)}\right) \Big/ \left(\frac{a}{\operatorname{mdc}(a,m)}\right) \end{aligned}$$

Mas $a/\operatorname{mdc}(a,m)$ e $m/\operatorname{mdc}(a,m)$ não tem fator comum (isto decorre da definição de MDC), portanto $a/\operatorname{mdc}(a,m)$ deve dividir k (*e este passo não seria possível se não tivéssemos feito a divisão por* $\operatorname{mdc}(a,m)$*!*). Seja

$$k' = \frac{k}{a/\operatorname{mdc}(a,m)}.$$

Então

$$\begin{aligned} b - c &= k'\frac{m}{\operatorname{mdc}(a,m)} \\ b &\equiv c \pmod{\frac{m}{\operatorname{mdc}(a,m)}} \end{aligned}$$

A recíproca é verificável fazendo o caminho reverso.
O caso particular listado no enunciado acontece quando $\operatorname{mdc}(a,m) = 1$, mas pode também ser demonstrado separadamente (é um exercício bastante simples, se for usada a definição de congruência). □

Teorema 6.7. $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, ..., $a \equiv b \pmod{m_k}$ *se e somente se* $a \equiv b \pmod{\operatorname{mmc}(m_1, m_2, \ldots, m_k)}$.

Demonstração. Se $a \equiv b \pmod{m_i}$ para $i = 1, \ldots, k$. Então

$$\begin{aligned} m_1 &\mid b - a, \\ m_2 &\mid b - a, \\ &\vdots \\ m_k &\mid b - a, \end{aligned}$$

ou seja, $b - a$ é múltiplo comum de todos os m_i, e portanto o MMC deles deve dividir $b - a$:

$$\begin{aligned} &\operatorname{mmc}(m_1, m_2, \ldots, m_k) \mid b - a \\ &a \equiv b \pmod{\operatorname{mmc}(m_1, m_2, \ldots, m_k)}. \end{aligned}$$

□

Teorema 6.8. *Sejam p e q primos. Se $a \equiv b \pmod{p}$ e $a \equiv b \pmod{q}$, então $a \equiv b \pmod{pq}$.*

Demonstração. Segue diretamente do Teorema 6.7, já que $\operatorname{mmc}(p, q) = pq$, porque p e q são primos.

□

O Lema 6.1, embora muito simples, nos permitirá trabalhar com inteiros negativos (em especial, -1) em congruências. Isto será útil em algumas demonstrações.

Lema 6.1. $m - 1 \equiv -1 \pmod{m}$.

Demonstração. Da definição de congruência,

$$\begin{aligned} (-1) - (m - 1) &= -1 - m + 1 \\ &= -m \end{aligned}$$

Mas $m \mid -m$, logo $m - 1 \equiv -1 \pmod{m}$. □

Lema 6.2. *Se p é primo, então todo número a tem inverso único módulo p, ou seja, existe $\overline{a}$ tal que $a\overline{a} \equiv 1 \pmod{p}$.*

Demonstração. Se p é primo, $\operatorname{mdc}(a, p) = 1$. Então, pelo Lema de Bézout, existem X, Y tais que

$$\begin{aligned} Xp + Ya &= 1 \\ Ya &= -Xp + 1 && (Ya \div p \text{ deixa resto } 1) \\ Ya &\equiv 1 \pmod{p}, \end{aligned}$$

e Y é o inverso de a módulo p.

Suponha que haja dois inversos de a, b e c ($ab \equiv 1 \pmod{p}$, e $ac \equiv 1 \pmod{p}$). Então

$$\begin{aligned} ab \equiv 1 \equiv ac \quad & \pmod{p} \\ ab \equiv ac \quad & \pmod{p} \\ b \equiv c \quad & \pmod{p} \qquad \text{(lei do cancelamento, } \operatorname{mdc}(a,p) = 1\text{)} \end{aligned}$$

Os inversos b e c, portanto, estão na mesma classe de congruência. □

Para computar o inverso de a módulo m, podemos usar o algoritmo estendido de Euclides.
Seja $a = 4$ e $m = 35$, co-primos. Para calcular $a^{-1} \pmod{21}$, calculamos os coeficientes de Bézout para os dois números e obtemos 9 e -1.

$$9(4) - 1(35) = 1.$$

Reescrevemos de forma a isolar $1 - 9(4)$:

$$\begin{aligned} 9(4) - 1(35) &= 1 \\ -1(35) &= 1 - 9(4) \\ 35 \mid 1 &- 9(4) \\ 1 &\equiv 9(4) \pmod{35} \end{aligned}$$

e claramente 9 é inverso de 4 módulo 35, já que o produto de ambos é congruente a um.
Se a e m não são co-primos, só podemos obter coeficientes de Bézout para $aX + mY = d$, com $d > 0$. Teremos, portanto um elemento a' tal que $aa' \equiv d \pmod{m}$, mas não um inverso para a.
Por exemplo, $\operatorname{mdc}(90, 220) = 10$. Se tentarmos obter o inverso de 90 móduilo 220, obteremos

$$\begin{aligned} 5(90) - 2(220) &= 10 \\ 5(90) - 10 &= 2(220) \\ 220 \mid 5(90) &- 10 \\ 5(90) &\equiv 10 \pmod{220}, \end{aligned}$$

e conseguimos $a' = 5$, mas $aa' = (90)(5) \equiv 10 \pmod{220}$, e não obtemos um inverso para 90 módulo 220.
Demonstraremos a seguir o Teorema de Wilson[4]; para isso o Lema 6.3 será necessário.

[4] Como muitos outros, este Teorema não carrega o nome de quem o demonstrou pela primeira vez. O que se conhece hoje como "Teorema de Wilson" foi usado por Ḥasan Ibn Al-Haytham (أبو علي، الحسن بن الحسن بن الهيثم), sem demonstração:

Lema 6.3. *Se* p *é primo,* $a^2 \equiv 1 \pmod{p}$ *se e somente se* $a \equiv \pm 1 \pmod{p}$.

Rashed, Roshdi. Ibn Al-Haytham et le théorème de Wilson. **Archive for History of Exact Sciences**, v. 22, n. 4, p. 305–321, 1980.

No artigo, Rashed aponta que

> *De fato mostraremos que numa obra cuja edição e tradução encontramos aqui, o famoso matemático e físico* ***Ibn Al-Haytham*** *(965-1040) apresenta durante sua solução de um problema de congruência linear o teorema de* ***Wilson*** *como uma proposição que expressa precisamente "uma propriedade necessária" dos números primos, em outras palavras, uma propriedade pertencente a eles "exclusivamente".*

No original,

> *Nous allons en effet montrer que dans un* Opuscule *dont on trouve ici même l'édition et la traduction, le célèbre mathématicien et physicien IBN AL-HAYTHAM (965-1040) présente au cours de sa solution d'un problème de congruences linéaires le théorème de WILSON comme une proposition exprimant précisément «une propriété nécessaire» des nombres premiers, autrement dit une propriété appartenant à ceux-ci «exclusivement».*

O teorema também foi conjecturado por Leibniz.

Vacca, Giovanni. Sui manoscritti inediti di Leibniz. **Bollettino di bibliografia e storia delle scienze matematiche**, v. 2, p. 113–116, 1899.

Aqui Vacca cita o original de Leibniz:

> *O produto de todos os inteiros precedendo um dado inteiro, quando dividido por esse inteiro, deixa resto um (ou complemento de um?) se o inteiro é primo. Se o inteiro é composto, deixa um número que tem fator comum com o inteiro, que é maior que um.*

No original,

> *Productus continuorum usque ad numerum qui antepraecedit datum divisus per datum relinquit 1 (vel complementum ad unum?) si datus sit primitivus. Si datus sit derivativus relinquet numerum qui cum dato habeat communem mensuram unitate majorem.*

Este mesmo trecho é citado por Giuseppe Peano, em uma publicação de 1897:

Peano, Giuseppe. Logique Mathématique. **Formulaire de Mathématiques**, 1897.

Pág. 85. Depois anunciado por Edward Waring, que afirmou em seu livro, *Meditationes Algebraicae*, que seu aluno John Wilson o havia descoberto (mas sem apresentar nenhuma prova).

Waring, Edward. **Meditationes Algebraicae**. 1. ed. [*S. l.*]: J. Archdeacon, 1770. Disponível em `https://archive.org/details/bim_eighteenth-century_meditationes-algebraicae_waring-edward-lucasian_1782`. Existem traduções para o Inglês.

Na página 218:

> *Seja* n *um número primo, e* $\frac{1\times2\times3\times4\cdots\overline{n-2}\times\overline{n-1}+1}{n}$ *será um número inteiro, e.g.* $\frac{1\times2+1}{3} = 1$, $\frac{1\times2\times3\times4+1}{5} = 5$, $\frac{1\times2\times3\times4\times5\times6+1}{7} = 103$, *etc. Esta propriedade muito elegante dos números primos foi descoberta pelo ilustríssimo homem, o grande especialista em matemática, o Armígero ("Squire", um título) John Wilson.*

No original,

> *Sit n numerus primus, &* $\frac{1\times2\times3\times4\cdots\overline{n-2}\times\overline{n-1}+1}{n}$ *erit integer numerus, e.g.* $\frac{1\times2+1}{3} = 1$, $\frac{1\times2\times3\times4+1}{5} = 5$, $\frac{1\times2\times3\times4\times5\times6+1}{7} = 103$, *&c. Hanc maxime elegantem primorum numerorum proprietatem invenit vir clariſſimus, rerum que mathematicarum peritiſſimus Joannes Wilſon Armiger.*

Demonstração.

$$
\begin{aligned}
& a^2 \equiv 1 \pmod{p} \\
& p \mid a^2 - 1 \\
& p \mid (a+1)(a-1) \\
& p \mid (a+1) \text{ ou } p \mid (a-1) && \text{(porque } p \text{ é primo)} \\
& a \equiv -1 \pmod{p} \text{ ou } a \equiv +1 \pmod{p}. && \square
\end{aligned}
$$

O teorema foi finalmente provado por Joseph-Louis Lagrange em 1770. Doze anos depois disso Waring publicou, em 1782, nova edição do *Meditationes*, desta vez creditando Lagrange.

Waring, Edward. **Meditationes Algebraicae**. 3. ed. [*S. l.*]: J. Archdeacon, 1782. Disponível em `https://archive.org/details/bim_eighteenth-century_meditationes-algebraic_waring-edward-lucasian_1770`. Existem traduções para o Inglês.

No prefácio, Waring menciona que

> *Também é dada uma demonstração elegante das propriedades dos números primos transmitidas no passado, viz. esse número* $1 \cdot 2 \cdot 3 \cdot 4 \cdots (n-1) + 1$ *será sempre divisível por n, se n for um número primo: uma demonstração elegante do teorema foi encontrada pela primeira vez por Lagrange.*

No original (Waring usa a grafia "Le Grange", versão latinizada de acordo com as regras da época. Lagrange era italiano descendente de franceses, nascido em Turim, com o nome Giuseppe Luigi Lagrangia,e posteriormente mudou para a França, adotando o nome Joseph-Louis Lagrange):

> *Datur etiam demonſtratio elegantis proprietatis primorum numerorum poſtea tradita, viz. quod numerus* $1 \cdot 2 \cdot 3 \cdot 4 \cdots (n-1) + 1$ *ſemper erit diviſibilis per* n*, ſi* n *ſit primus numerus : bujuſce theorematis demonſtrationem elegantem prius invenit Le Grange.*

Nessa terceira edição, no entanto, Waring ainda manteve a menção a Wilson como o "primeiro a descobrir o teorema" (o texto que se refere a Wilson foi mantido, sem mudanças). Um breve comentário sobre a história do teorema é dado por Oystein Ore:

Ore, Oystein. **Number Theory and Its History**. New York: Dover Publications, 1976.

O capítulo 11 discute a história e desenvolvimento do teorema, inclusive uma generalização feita por Gauss (Gauß) no *Disquisitiones* (Gauss mostrou que há como generalizá-lo para módulos compostos).

Um exemplo simples: para $p = 11$, os quadrados são

x	x^2	$\pmod{11}$
0	0	0
1	1	1
2	4	4
3	9	9
4	16	5
5	25	3
6	36	3
7	49	5
8	64	9
9	81	4
10	100	1

Somente 1 e 10 tem quadrado congruente a um módulo 11 (e $10 \equiv -1 \pmod{11}$).

Teorema 6.9 (de Wilson)**.** p *é primo se e somente se* $(p-1)! \equiv -1 \pmod{p}$.

Demonstração. Suponha que n é composto; provaremos que $(n-1)! \not\equiv -1 \pmod{n}$. Se n é composto, existe algum q natural, $2 \leq q \leq n-2$, tal que $q \mid n$. Seja então $n = kq$. Suponha que $(n-1)! \equiv -1 \pmod{n}$.

$$\begin{aligned}
(n-1)! &\equiv -1 \pmod{n} \\
(n-1)! &= rn - 1 && \text{(para algum } r \in \mathbb{Z}\text{)} \\
&= rkq - 1 \\
&= q(rk) - 1 \\
(n-1)! &\equiv -1 \pmod{q}
\end{aligned}$$

Mas como $2 \leq q \leq n-2$, q é um dos fatores em $(n-1)!$, e $q|(n-1)!$, portanto $(n-1)! \equiv 0 \pmod{q}$ – uma contradição, e este caso não pode acontecer.

Agora passamos ao caso em que p é primo, e provaremos que $(p-1)! \equiv -1 \pmod{p}$. Pelo Lema 6.2 existe um único b tal que $ab \equiv 1 \pmod{p}$. De todos os números entre 1 e $p-1$, os únicos que são seus próprios inversos são 1 e $p-1$ (Lema 6.3[5]). Os outros (ou seja, $2, 3, \ldots, p-2$) podem ser agrupados

[5] **Lema 6.3: Se** p **é primo,** $a^2 \equiv 1 \pmod{p}$ **se e somente se** $a \equiv \pm 1 \pmod{p}$**.**

em pares:

$$\begin{aligned}
\overbrace{(a_1\overline{a_1})}^{\equiv 1}\overbrace{(a_2\overline{a_2})}^{\equiv 1}\cdots\overbrace{(a_k\overline{a_k})}^{\equiv 1} &\equiv 1 \pmod{p} && \\
2\cdot 3\cdot 4\cdots(p-2) &\equiv 1 \pmod{p} && (a_k \text{ são } 2\cdot 3\cdots n-2)\\
1\cdot 2\cdot 3\cdot 4\cdots(p-2) &\equiv 1 \pmod{p} && (\times 1)\\
1\cdot 2\cdot 3\cdot 4\cdots(p-2)(p-1) &\equiv p-1 \pmod{p} && (\times[p-1])\\
(p-1)! &\equiv -1 \pmod{p} && (p-1\equiv -1 \pmod{p})
\end{aligned}$$

Isto completa a demonstração. □

Para construir um exemplo, escolhemos um primo: 7. Pelo Teorema de Wilson,

$$(7-1)! = 720 \equiv -1 \pmod{7},$$

que verificamos usando a definição de congruência: $7 \mid 720-(-1)$. De fato, $721/7 = 103$.

6.2 Aplicação: critérios de divisibilidade

Uma aplicação simples de congruências é na demonstração de critérios usados para determinar se inteiros são divisíveis[6] por 2, 3, 4, 5, 9, 10 e 11.

Teorema 6.10. *Um inteiro é par se e somente se seu último dígito (o menos significativo) é par.*

Demonstração.

$$\begin{aligned}
10 &\equiv 0 \pmod{2}\\
10^k \equiv 0^k &\equiv 0 \pmod{2}
\end{aligned}$$

Portanto

$$\begin{aligned}
x &\equiv d_0 + 10d_1 + 10^2 d_2 + \cdots + 10^n d_n \pmod{2}\\
&\equiv d_0 \pmod{2}
\end{aligned}$$

Assim, n é par se seu último dígito for par. □

[6] Muitos desses critérios já existiam antes da consolidação do conceito de congruência. Os babilônios (com seu sistema de base 60) tinham critérios de divisibilidade por 2, 3, 4, 5 e 6. Os egípcios (com base dez), por 2, 3, 4, 5 e 10. Há registros também de que na Índia, Āryabhaṭa (आर्यभटः, 476-550) e Brahmagupta (ब्रह्मगुप्तः, 598-668) teriam desenvolvido critérios de divisibilidade por 7, 8 9 e 11. O uso de congruências torma sistemática a descrição desses critérios, resumindo muitas regras específicas em uma teoria compacta e simples, aplicável a diferentes bases numéricas.

Teorema 6.11. $3 \mid n$ *se e somente se seu a soma dos dígitos de* n *é divisível por* 3*;* $9 \mid n$ *se e somente se seu a soma dos dígitos de* n *é divisível por* 9*.*

Demonstração.

$$\begin{aligned} 10 &\equiv 1 && \pmod 3 \\ 10^k &\equiv 1^k \equiv 1 && \pmod 3 \end{aligned}$$

Portanto

$$\begin{aligned} x &\equiv d_0 + 10d_1 + 10^2 d_2 + \cdots + 10^n d_n && \pmod 3 \\ &\equiv d_0 + (9d_1 + d_1) + (99d_2 + d_2) + \cdots + (99\cdots 9d_n + d_n) && \pmod 3 \\ &\equiv \left(d_0 + d_1 + d_2 + \cdots + d_n\right) \ + \ \left(9d_1 + 99d_2 + \cdots + 99\cdots 9d_n\right) && \pmod 3 \\ &\equiv \left(d_0 + d_1 + d_2 + \cdots + d_n\right) && \pmod 3 \end{aligned}$$

Mudando o módulo para 9 obtemos o resultado para $9 \mid n$. □

Teorema 6.12. $11 \mid n$ *se e somente se a soma de seus dígitos, alternando sinal, é divisível por* 11*.*

Demonstração.

$$\begin{aligned} 10 &\equiv -1 && \pmod{11} \\ 10^k &\equiv (-1)^k && \pmod{11} \end{aligned}$$

Portanto

$$\begin{aligned} x &\equiv d_0 + 10d_1 + 10^2 d_2 + \cdots + 10^n d_n && \pmod{11} \\ &\equiv d_0 + (-1)d_1 + (-1)^2 d_2 + \cdots + (-1)^n d_n && \pmod{11} \\ &\equiv d_0 - d_1 + d_2 - \cdots + (-1^n)d_n && \pmod{11} \end{aligned}$$

□

O Exercício 143 pede a demonstração de mais alguns critérios de divisibilidade.

Teorema 6.13. *Para todo inteiro positivo* n*,*

(i) $4 \mid n$ *se e somente se seus dois últimos dígitos representam um número divisível por* 4*.*

(ii) $5 \mid n$ *se e somente se seu último dígito é* 0 *ou* 5*.*

(iii) $10 \mid n$ *se e somente se seu último dígito é zero.*

Para divisores que sejam números compostos por estes estudados nesta seção, basta usar simultaneamente critérios de divisibilidade: um número é divisível por 12 se e somente se é divisível por 3 e por 4, logo a soma de seus dígitos deve ser divisível por 3, *e* seus dois últimos dígitos devem representar um número divisível por 4.

Questionamos, evidentemente, sobre um critério de divisibilidade por sete. O método acima pode nos dar um critério, mas ele não é prático.

$$\begin{aligned} 10 &\equiv 3 && \pmod 7 \\ 10^k &\equiv 3^k && \pmod 7 \\ x &\equiv d_0 + 3d_1 + 3^2 d_2 + \cdots + 3^n d_n && \pmod 7 \end{aligned}$$

Assim, o que podemos dizer é que n é divisível por sete se e somente se a soma ponderada de seus dígitos, $d_0 + 3d_1 + 3^2 d_2 + \cdots + 3^n d_n$, é divisível por sete.

6.2.1 Em bases diferentes

O que fizemos para determinar critérios de divisibilidade na base dez foi buscar divisores d tais que $10 \equiv \pm 1 \pmod d$ ou $10 \equiv 0 \pmod d$. O mesmo vale para outras bases: se o divisor é d e a base é b, obteremos um critério de divisibilidade útil quando

$$b \equiv 0 \pmod d, \quad b \equiv +1 \pmod d, \quad b \equiv -1 \pmod d.$$

Exemplificamos com a base oito.

Teorema 6.14. *Na base oito,*

(i) $8 \mid n$ *se e somente se o último dígito de* n *é zero;*

(ii) $7 \mid n$ *se e somente se a soma dos dígitos de* n *é divisível por sete;*

(iii) $9 \mid n$ *se e somente se a soma alternada dos dígitos de* n *é divisível por nove.*

Demonstração.
(i)

$$\begin{aligned} 8 &\equiv 0 && \pmod 8 \\ 8^k &\equiv 0 && \pmod 8 \end{aligned}$$

Portanto

$$\begin{aligned} x &\equiv d_0 + 8d_1 + 8^2 d_2 + \cdots + 8^n d_n && \pmod 8 \\ &\equiv d_0 && \pmod 8 \end{aligned}$$

(ii)

$$\begin{aligned} 8 &\equiv 1 && \pmod 7 \\ 8^k &\equiv 1 && \pmod 7 \end{aligned}$$

Portanto

$$\begin{aligned} x &\equiv d_0 + 8d_1 + 8^2 d_2 + \cdots + 8^n d_n && \pmod 7 \\ &\equiv d_0 + d_1 + d_2 + \cdots + d_n && \pmod 7 \end{aligned}$$

(iii)

$$\begin{aligned} 8 &\equiv -1 && \pmod 9 \\ 8^k &\equiv (-1)^k && \pmod 9 \end{aligned}$$

Portanto

$$\begin{aligned} x &\equiv d_0 + 8d_1 + 8^2 d_2 + \cdots + 8^n d_n && \pmod 9 \\ &\equiv d_0 + (-1)d_1 + (1)d_2 + \cdots + (-1)^n d_n && \pmod 9 \\ &\equiv d_0 - d_1 + d_2 - \cdots + (-1)^n d_n && \pmod 9 \end{aligned}$$

□

6.3 Congruências Lineares e Equações Diofantinas

Equações Diofantinas são equações polinomiais onde os coeficientes são inteiros – e onde se procuram soluções inteiras[7]. Uma equação Diofantina

[7] O nome é referência a Diofanto de Alexandria, matemático que viveu no século III, e que estudou estas equações. Um livro com os estudos de Diofanto, com título "Arithmetica" (*Αριθμητικά*), tornou-se estímulo para muitos matemáticos europeus nos séculos seguintes. Tome, por exemplo, a conhecida história do último teorema de Fermat: a margem que Fermat declarou que era muito pequena para conter sua demonstração era de um exemplar deste livro. Boa parte dos treze livros de Diofanto, infelizmente, se perderam: há livros faltando, e o texto original, em grego, se perdeu, e o que se conhece hoje é uma tradução do Grego para o Árabe, que depois foi traduzido de volta para Grego e Latim. O volume que Fermat usava é

muito conhecida é $a^n + b^n = c^n$, que de acordo com o último Teorema de Fermat não tem soluções inteiras. Nesta seção desenvolvemos uma técnica simples para determinar soluções para o tipo mais simples de equações Diofantinas – as lineares.

Definição 6.2. *Uma equação polinomial* $p(x) = 0$ *com coeficientes inteiros é chamada de* ***equação Diofantina****. Uma equação Diofantina é* ***linear*** *se o grau do polinômio* p *é um.* ◀

Nesta seção estudamos somente as equações diofantinas lineares, da forma $ax + by = c$.
Sabemos que $ax + by = c$ (ou, equivalentemente, a congruência $ax \equiv c \pmod{b}$) tem solução se e somente se $\operatorname{mdc}(a, b) = d \mid c$, Para resolver a equação, primeiro a simplificamos, dividindo-a por d:

$$Ax + By = C, \quad A = \frac{a}{\operatorname{mdc}(a,b)}, B = \frac{b}{\operatorname{mdc}(a,b)}, C = \frac{c}{\operatorname{mdc}(a,b)}$$

Agora temos $\operatorname{mdc}(A, B) = 1$. Considere a equação

$$Ar + Bs = 1.$$

Podemos facilmente encontrar uma solução para ela usando o algoritmo de Euclides para o MDC: basta calcular o MDC de A e B; chegaremos a uma equação da forma $\alpha\beta + \gamma\delta = 1$.
Posteriormente, multiplicamos a equação e sua solução por C:

$$ArC + BsC = C,$$

e temos uma solução para a equação original.

Exemplo 6.5. *Resolveremos a equação* $15x+51y = 42$*. Como* $\operatorname{mdc}(15, 51) = 3$ *e* $3 \mid 42$*, as soluções que procuramos são as mesmas de*

$$5x + 17y = 14.$$

uma edição publicada por Bachet em 1621.
Os dois volumes a seguir, em Latim e Grego e publicados por Paul Tannery em 1895, contém parte dos volumes originais (sabe-se que há tres volumes faltando, mas não se sabe quais):

Diophantus. **Diophanti Alexandrini opera omnia cum Graecis commentariis**. Edição: P. Tannery. [*S. l.*]: Stutgardiae Teubner, 1895. v. 1. Disponível em `https://archive.org/details/diophantialexan03plangoog/`.

Diophantus. **Diophanti Alexandrini opera omnia cum Graecis commentariis**. Edição: P. Tannery. [*S. l.*]: Stutgardiae Teubner, 1895. v. 2. Disponível em `https://archive.org/details/diophantialexan00plangoog`.

Há uma tradução de Thomas Heath para o Inglês, de 1910, baseada no trabalho de Tannery:

Heath, Thomas L. **Diophantus Of Alexandria A Study In The History Of Greek Algebra**. [*S. l.: s. n.*], 1910. Disponível em `https://archive.org/details/in.ernet.dli.2015.154147`.

Agora resolvemos $5x' + 17y' = 1$. *Calculamos* $\mathrm{mdc}\,(17, 5)$ *e obtemos os coeficientes de Bézout:*

$$5(7) + 17(-2) = 1.$$

Temos as soluções $x' = 7, y' = -2$. *Multiplicando por* 14 *obtemos*

$$x = 98, \quad y = -28.$$

Finalmente, verificamos facilmente que $5(98) + 17(-28) = 14$.
Esta é, no entanto, somente uma das infinitas soluções para a equação. Se $ax + by = c$, *então também é verdade que* $a(x + kb) + b(y - ka) = c$, *para todo* $k \in \mathbb{Z}$:

$$\begin{aligned} a(x + kb) + b(y - ka) &= c \\ ax + kab + by - kab &= c \\ ax + by &= c \end{aligned}$$

Para determinarmos a forma geral da solução, precisamos calcular

$$\begin{aligned} a(x + bk) + b(y - ak) &= 42 \\ 15(x + 51k) + 51(y - 15k) &= 42 \\ 15(98 + 51k) + 51(-28 - 15k) &= 42. \end{aligned}$$

Na última linha, usamos $x + kb = 98 + 51k$, $y + ka = -28 - 15k$. *As soluções são os pares* (x, y) *no conjunto*

$$\{(98 + 51k, -15k - 28) \mid k \in \mathbb{Z}\}. \qquad \blacktriangleleft$$

Exemplo 6.6. *A equação diofantina* $6x + 4y = 25$ *não tem soluções, porque* $\mathrm{mdc}\,(6, 4) = 2$, *e* $2 \nmid 25$. $\blacktriangleleft$

Exemplo 6.7. *Queremos todas as soluções para* $6x + 10y = 164$, *com uma restrição adicional:* $x, y \geq 9$.
As soluções serão as mesmas para

$$3x + 5y = 82,$$

portanto calculamos o MDC e os coeficientes de Bézout para 3 *e* 5:

$$3(2) + 5(-1) = 1$$

Multiplicamos por 82, *e obtemos*

$$3(164) + 5(-82) = 82.$$

Esta solução ainda não é uma das que queremos, porque $y = -82 < 9$. *A*

forma geral é, no entanto,

$$3(164 + 5k) + 5(-82 - 3k) = 82$$

e as soluções que queremos são

$$164 + 5k \geq 9 \quad \text{(i)}$$
$$-82 - 3k \geq 9 \quad \text{(ii)}$$

Resolvemos (i)*:*

$$5k \geq 9 - 164$$
$$k \geq -\frac{155}{5} = -31$$

E agora, (ii)*:*

$$-3k \geq 82 + 9$$
$$k \leq -\frac{91}{3} \approx -30.333$$

Assim, somente podemos usar $k = -31$*.* ◀

A equação diofantina $ax - my = b$ é claramente equivalente à congruência linear $ax \equiv b \pmod{m}$, que tem infinitas soluções (quando há alguma). No entanto, podemos afirmar algo a respeito da quantidade de soluções incongruentes módulo m.

Teorema 6.15. *A congruência* $ax \equiv b \pmod{m}$ *tem* $d = \operatorname{mdc}(a, m)$ *soluções incongruentes módulo* m *se e somente se* $d \mid b$*. Se* $d \nmid b$*, então não há soluções.*

Demonstração. Seja $d = \operatorname{mdc}(a, m)$. Como a equação Diofantina $ax - my = b$ tem soluções se e somente se $d \mid b$, precisamos apenas mostrar que há d soluções incongruentes módulo m.

Se $d \mid b$, reescrevemos a equação dividindo todos por d:

$$Ax \equiv B \pmod{M}, \quad A = \frac{a}{d}, B = \frac{b}{d}, M = \frac{m}{d}.$$

Como agora A e M são co-primos, existe um único inverso para A módulo M, que denotaremos $\overline{A}$. Temos portanto $A\overline{A} \equiv 1 \pmod{M}$. Suponha que

tenhamos uma solução x_0:

$$\begin{aligned}
Ax_0 &\equiv B \pmod{M} \\
\overline{A}Ax_0 &\equiv \overline{A}B \pmod{M} && (\overline{A} \text{ unicamente determinado}) \\
x_0 &\equiv \overline{A}B \pmod{M} \\
M &\mid \overline{A}B - x_0 \\
kM &= \overline{A}B - x_0 && (k \text{ unicamente determinado}) \\
x_0 &= \overline{A}B - kM,
\end{aligned}$$

uma única solução para $Ax \equiv B \pmod{M}$. Passamos agora para módulo m. Suponha que a solução para $Ax \equiv B \pmod{M}$ seja x_0. As soluções para esta congruência seriam

$$x_0 + tM, \quad \text{com } t = 0, 1, \ldots, M-1.$$

Mas há somente uma, porque ao somar "$+tM$", não estamos mudando a solução módulo M.

No entanto, se olhamos para as mesmas soluções módulo m teremos:

$$x_0 + tM, \quad \text{com } t = 0, 1, \ldots, m-1.$$

Como as soluções são espaçadas por M, teremos $m/M = d$ possibilidades incongruentes. □

Exemplo 6.8. *Resolveremos* $396x \equiv 729 \pmod{27}$.

Como $\operatorname{mdc}(396, 27) = 9$ *e* $9 \mid 729$*, dividimos a equação por* 9*:*

$$44x \equiv 81 \pmod{3}.$$

Como 44 *é co-primo com* 3*, tem inverso:* $(44)(8) \equiv 1 \pmod{3}$*, e*

$$\begin{aligned}
(44)(8)x &\equiv (8)(81) && \pmod{3} \\
x &\equiv 648 && \pmod{3} \\
3 &\mid 648 - x \\
3k &= 648 - x \\
x &= 3k + 648
\end{aligned}$$

Temos 9 *valores de* k *que são incongruentes módulo* 27*. Estes nos darão as*

9 soluções:

k	$9k + 648$	$(\mathrm{mod}\ 27)$
0	648	0
1	651	3
2	654	6
3	657	9
4	660	12
5	663	15
6	666	18
7	669	21
8	672	24
9	675	0
10	678	3
⋮	⋮	⋮

As nove primeiras linhas mostram os nove valores incongruentes. Na décima (para $k = 9$), a sequência começa a se repetir. ◀

6.4 O Teorema Chinês dos Restos

Já tratamos de como resolver congruências lineares em uma variável. Agora consideramos como resolver um sistema de congruências lineares simultâneas.

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

O problema de resolver congruências simultâneas foi estudado bastante cedo na História da Matemática. A referência usual em textos de Matemática contemporânea[8] é o texto Sūnzǐ Suànjīng (孫子算經, "O Clássico

[8] Āryabhaṭa [9] (476-550), Al-Khwarizmi– خوارزمی –[10], Ibn Yunus– ابن یونس –[11], Ḥasan Ibn Al-Haytham – أبو علي، الحسن بن الحسن بن الهيثم –[12], Bhāskara भास्कर[13], Yī Xíng 一行 [14], Qín Jiǔsháo [15](秦九韶, 1202-1261) e muitos europeus escreveram sobre o mesmo problema – uma longa lista de matemáticos é dada por Dickson.

Dickson, Leonard Eugene. **History of The Theory of Numbers**. New York, N.Y.: Chelsea Publishing Company, 1971. v. 2.

[15] O nome completo é Abū Jaᶜfar Muḥammad ibn Mūsā al-Khwārizmī , ابو جعفر محمد بن موسى خوارزمی.

Matemático do Mestre Sūn ")[16], escrito por Sūnzǐ [21] (孫子, "Mestre Sūn "), que no Século IV teria proposto problemas como o que segue, apresentando

[16]O livro tem três capítulos, e o Teorema que descrevemos aqui é apresentado (de maneira bastante diferente, mais limitada e na forma de solução para problema concreto) no capítulo 3. Há uma tradução para o Inglês, de Lam Lay Yong e An Tian Se.

Yong, Lam Lay; **Se**, An Tian. **Fleeting Footsteps**. [*S. l.*]: World Scientific Publishing Company, 2004.

O livro traz, além da tradução do clássico do Mestre Sūn , comentários sobre o contexto em que surgiu – aspectos socioeconômicos e considerações sobre a possibilidade do sistema Hindu-Árabe de numerais ter tido origens na China. O original do Mestre Sūn é escrito na forma problema-resposta-método. Por exemplo, o quarto problema do terceiro livro é

> *Agora, há um livro sobre Budismo com um total de 29 Capítulos. Cada Capítulo tem 63 caracteres. Encontre o número total de caracteres.*
> *Resposta:* 1827.
> *Método: Tome 29 capítulos e multiplique por 63 caracteres para obter a resposta.*

Este é um problema básico, mas exemplifica o estilo. Aspectos culturais se entrelaçam com a Matemática (a separação das Ciências Exatas do resto da cultura é um fenômeno essencialmente europeu, consequência do Iluminismo). O último problema do livro é:

> *Agora, há uma mulher grávida cuja idade é 29. Se o período de gestação é de nove meses. determine o sexo da criança que nascerá.*
> *Resposta: masculino.*
> *Método: Tome 49, some o período da gestação e subtraia a idade. Do resto remova 1 representando o céu, 2 a terra, 3 o homem, 4 as quatro estações, 5 as 5 fases*[17]*, 6 as seis flautas de afinação*[18]*, 7 as sete estrelas*[19]*, 8 os oito ventos e 9 as nove divisões (da China sob Yu, o Grande)*[20]*. Se o resto for ímpar, será masculino, e se o resto for par, será feminino.*

Para além das crenças presentes no método, é interessante que Mestre Sūn não tenha simplificado a conta, já que $49-1-2-3-4-5-6-7-8-9=4$, que é par, e não modifica a paridade da idade – a resposta poderia ser "Se a idade prevista para o nascimento (29 mais o período de gestação) é ímpar, será masculino; se é par, será feminino". Os elementos citados (céu, terra, etc) tinham grande peso cultural, e aparentemente este problema foi concebido mais para apresentar (ou citar) estes elementos do que realmente para tratar de algum método matemático.

[17]Cinco fases são os cinco elementos, madeira, fogo, terra, metal e água, de grande importancia na filosofia tradicional chinesa.

[18]"Nove divisões", ou "nove províncias" é uma referência à divisão da China antiga em nove regiões. Na tradição chinesa, diz-se que Yu, o Grande (大禹) teria dividido a China em nove províncias (zhōu , 州, literalmente "terra"). Não há evidências de que o Grande Yu de fato tenha existido.

[19]As seis flautas de afinação eram um conjunto de tubos de bambu ou metal, que produziam seis notas musicais, e além de serem fundamentais para a música tradicional chinesa, tinham um significado filosófico, representando harmonia e equilíbrio.

[20]As sete estrelas da constelação Ursa Maior.

[21]Homônimo, mas absolutamente não o mesmo Sūnzǐ (544 a.C - 496 a.C) que escreveu "A Arte da Guerra" (e cujo nome é usualmente transliterado como "Sun Tzu", e cuja existência é questionada por historiadores).

Sun Tzu. **A Arte da Guerra**. [*S. l.*]: Edipro, 2021. Sun é nome; Tzu é título (mestre). Edição bilíngue. Há também uma tradução para o Inglês, livremente disponível em `https://archive.org/details/in.gov.ignca.18750/page/115/mode/2up`.

O Sūnzǐ que expôs o Teorema Chinês viveu muito mais tarde que o autor do clássico livro sobre a Guerra (presumindo que este existiu!). Infelizmente não sabemos muito sobre o Matemático Mestre Sūn , a não ser que viveu entre os séculos III e V, na dinastia Tang.

também um “método” para resolvê-lo:

> *“Há certas coisas cuja quantidade é desconhecida. Repetidamente divididas por 3, o resto é 2; por 5, o resto é 3; e por 7 o resto é 2. Qual é a quantidade?”* [22]

O problema dado por Sūnzǐ circulou por toda a China, e havia interesse dos matemáticos em uma solução geral para problemas do mesmo tipo (isoladamente, o problema era somente um quebra-cabeças interessante). A primeira vez em que o teorema foi de fato provado na China foi em 1247, por Qín Jiǔsháo 秦九韶 [23] no “Tratado Matemático em Nove Seções” (Shùshū Jiǔzhāng , 数书九章)[24]. O problema de resolver sistemas de equa-

[22] Este é o vigésimo-sexto problema da terceira parte do livro de Sūnzǐ .

Yong, Lam Lay; **Se**, An Tian. **Fleeting Footsteps**. [*S. l.*]: World Scientific Publishing Company, 2004.

A resposta dada pelo Mestre é

> *Resposta: 23.*
> *Método: Se contarmos aos três e restam 2, tome 140. Se contarmos aos cinco e restam 3, tome 63. Se contarmos aos sete e restam 2, tome 30. Some-os para obter 233, e subtraia 210 para obter a resposta.*

O texto original, com a resposta e o método:

> 今有物，不知其數。三、三數之，賸二；五、五數之，賸三；七、七數之，賸二。問物幾何 ？
> 答曰：二十三。
> 術曰：「三、三數之，賸二」，置一百四十；「五、五數之，賸三」，置六十三；「七、七數之，賸二」，置三十。并之，得二百三十三。以二百一十減之，即得。凡三、三數之，賸一，則置七十；五，五數之，賸一，則置二十一；七、七數之，賸一，則置十五。一百六以上，以一百五減之，即得。
> *(Jīn yǒu wù, bùzhī qí shù. Sān, sān shù zhī, shèng èr; wǔ, wǔ shù zhī, shèng sān; qī, qī shù zhī, shèng èr. Wèn wù jǐhé?*
> *dá yuē: Èrshísān*
> *shù yuē:`Sān, sān shù zhī, shèng èr', zhì yībǎi sìshí;`wǔ, wǔ shù zhī, shèng sān', zhì liùshísān;`qī, qī shù zhī, shèng èr', zhì sānshí. Bìng zhī, dé èrbǎi sānshísān. Yǐ èrbǎi yīshí jiǎn zhī, jí dé. Fán sān, sān shù zhī, shèng yī, zé zhì qīshí; wǔ, wǔ shù zhī, shèng yī, zé zhì èrshíyī; qī, qī shù zhī, shèng yī, zé zhì shíwǔ. Yībǎi liù yǐshàng, yǐ yībǎi wǔ jiǎn zhī, jí dé.)*

[23] Qín Jiǔsháo (1202-1261), Chinês.

[24] A primeira das nove seções se chama “Dayan lei” (大衍類 ou 大衍类). Um tratado sobre Qín Jiǔsháo e suas contribuições é a tese de mestrado de Ke-Xin Au Yong.

Yong, Ke-Xin Au. **Qin Jiushao and His Mathematical Treatise in Nine Sections in Thirteenth-Century China**. 2011. Diss. (Mestrado) – University of Alberta.

Detalhes do método desenvolvido por Qín Jiǔsháo são dados no livro de Ulrich Libbrecht e no capítulo de Dauben.

Libbrecht, Ulrich. **Chinese Mathematics in the Thirteenth Century: the Shu-shu chiu-chang of Ch’in Chiu-shao**. [*S. l.*]: MIT, 1973.

Dauben, Joseph W. Mathematics of Egypt, Mesopotamia, China, India, and Islam: A Sourcebook. *In:* edição: Victor Katz. [*S. l.*]: Princeton University Press, 2007. Chinese Mathematics.

ções envolvendo restos está também presente no tratado Brāhmasphuṭa-siddhānta (ब्रह्मस्फुटसिद्धान्तः), do Indiano Brahmagupta (ब्रह्मगुप्तः, 598-668)[25], que era astrônomo – problemas deste tipo surgem naturalmente ao se tratar de corpos celestiais com órbitas de períodos diferentes[26].

Enunciamos o Teorema a seguir, e damos uma demonstração construtiva (o método que derivamos da demonstração é bastante diferente do de Sūnzǐ).

Teorema 6.16 (Chinês dos restos)**.** *Sejam* $m_1, m_2, \ldots, m_r$ *inteiros co-primos entre si. Então o sistema de congruências*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

tem solução única módulo $M = m_1 m_2 \cdots m_r$*, para quaisquer* $a_1, a_2, \ldots, a_r$*.*

Demonstração. Para $k = 1, 2, \ldots, r$, defina

$$M_k = \frac{M}{m_k}.$$

Então $\operatorname{mdc}(M_k, m_k) = 1$ para todo k, porque os m_k são co-primos, e de M_k retiramos o fator m_k. Como M_k e m_k são co-primos, então *existe inverso de* M_k *módulo* m_k.

Agora, para cada M_k, denote $\overline{M_k}$ como o inverso de M_k módulo m_k. Ou seja,

$$M_k \overline{M_k} \equiv 1 \pmod{m_k}.$$

A solução do sistema é

$$x \equiv a_1 M_1 \overline{M_1} + a_2 M_2 \overline{M_2} + \cdots + a_r M_r \overline{M_r} \pmod{M}. \tag{6.1}$$

[25] **Brahmagupta**. **Brahmasphuta Siddhanta (Brāhmasphuṭasiddhānta)**. [*S. l.: s. n.*].

[26] No início da questão sete do Brāhmasphuṭasiddhānta :

> *Aquele que encontra o ciclo (yuga) e assim por diante, de dois, três, quatro ou mais planetas, a partir dos respectivos ciclos passados dos planetas dados, conhece o método do pulverizador.*

Colebrooke, Henry Thomas. **Algebra, with Arithmetic and mensuration, from the Sanscrit of Brahmegupta and Bháscara**. [*S. l.*]: London J. Murray, 1817. Disponível em https://archive.org/details/algebrawitharith00brahuoft.

Justificamos. Note que na soma acima, para $i \neq j$,

$$\begin{aligned} a_i M_i \overline{M_i} &\equiv 0 \pmod{m_j} && \text{(porque } m_j \mid M_i\text{)} \\ a_i M_i \overline{M_i} &\not\equiv 0 \pmod{m_i} && \text{(porque } m_i \nmid M_i\text{)} \end{aligned}$$

e portanto $a_i M_i \overline{M_i} \equiv (a_i)(0)(\overline{M_i}) \equiv 0 \pmod{m_j}$.
Assim, para cada m_i a soma será

$$\begin{aligned} x &\equiv a_1(0)\overline{M_1} + a_2(0)\overline{M_2} + \cdots + a_i M_i \overline{M_i} + \cdots + a_r(0)\overline{M_r} && \pmod{m_i} \\ &\equiv a_i M_i \overline{M_i} && \pmod{m_i} \\ &\equiv a_i && \pmod{m_i} \end{aligned}$$

A última linha é válida porque $M_i \overline{M_i} \equiv 1 \pmod{m_i}$.
Conseguimos então x que é congruente a cada um dos a_i módulo m_i, e que é único módulo M (porque o definimos como classe de congruência módulo M, na equação 6.1). □

Exemplo 6.9. *Resolveremos o sistema*

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 1 \pmod{7} \\ x &\equiv 3 \pmod{10} \end{aligned}$$

Temos $M = (3)(7)(10) = 210$, *e*

$$\begin{aligned} M_1 &= (7)(10) = 70 \\ M_2 &= (3)(10) = 30 \\ M_3 &= (3)(7) = 21 \end{aligned}$$

Os inversos são

$$\begin{aligned} \overline{M_1} &= 1 \pmod{3} \\ \overline{M_2} &= 4 \pmod{7} \\ \overline{M_3} &= 1 \pmod{10} \end{aligned}$$

Assim,

$$\begin{aligned} x &\equiv 2(70)(1) + 1(30)(4) + 3(21)(1) \\ &\equiv 323 \\ &\equiv 113 \pmod{210} \end{aligned}$$

A solução do sistema é $x \equiv 113 \pmod{210}$*, como podemos verificar:*

$$\begin{aligned} 113 &\equiv 2 \pmod{3} \\ 113 &\equiv 1 \pmod{7} \\ 113 &\equiv 3 \pmod{10} \end{aligned}$$

Note que toda a classe de congruência 113 *módulo* 210 *é solução para o sistema:* $\{\ldots, -307, -97, 113, 323, 533, \ldots\} = \{210k + 113 \mid k \in \mathbb{Z}\}$. ◀

6.4.1 Módulos não co-primos

O Teorema Chinês dos Restos pode ser generalizado para sistemas onde os módulos não são co-primos, mas sistemas dessa forma nem sempre tem solução. Nesta seção detalhamos o critério para existência da solução, além de uma demonstração construtiva que permite obte-la, quando existir.
Nos Lemas a seguir trataremos de sistemas de congruências

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_k \pmod{m_k}. \end{aligned} \tag{6.2}$$

Lema 6.4. *Se, para algum* $i \neq j$*,* $\operatorname{mdc}(m_i, m_j) \nmid (a_i - a_j)$*, então o sistema de congruências 6.2 não tem solução.*

Demonstração. Se $\operatorname{mdc}(m_i, m_j) \nmid (a_i - a_j)$, então

$$a_i \not\equiv a_j \pmod{\operatorname{mdc}(m_i, m_j)},$$

mas isso significa que x não pode satisfazer simultaneamente as duas equações

$$\begin{aligned} x &\equiv a_i \pmod{\operatorname{mdc}(m_i, m_j)}, \\ x &\equiv a_j \pmod{\operatorname{mdc}(m_i, m_j)}. \end{aligned}$$

porque se fosse o caso teríamos $a_i \equiv a_j \pmod{\operatorname{mdc}(m_i, m_j)}$. □

Lema 6.5. *Se, para todo* $i \neq j$*,* $\operatorname{mdc}(m_i, m_j) \mid (a_i - a_j)$*, então o sistema de congruências 6.2 tem solução.*

Demonstração. Em cada congruência $x \equiv a_i \pmod{m_i}$, denotamos a fatoração de m_i por $m_i = p_1^{i_1} p_2^{i_2} \cdots$ (ou seja, $p_1, p_2, \ldots$ são todos os primos, e $i_1, i_2, \ldots$ são os expoentes dos primos na fatoração de m_i – note que somente alguns dos primos terão expoente diferente de zero). Agora, troca-

mos cada uma destas congruências da forma $x \equiv a_i \pmod{m_i}$ por um conjunto de congruências, substituindo m_i em cada uma por uma das potências de primo na fatoração de m_i. Trocamos

$$x \equiv a_i \pmod{m_i}$$

por

$$\begin{aligned} x &\equiv a_i \pmod{p_1^{i_1}} \\ x &\equiv a_i \pmod{p_2^{i_2}} \\ &\vdots \\ x &\equiv a_k \pmod{p_k^{i_k}}. \end{aligned}$$

Como exemplo, se a congruência original é

$$x \equiv 3 \pmod{175},$$

teremos $m = 175 = 5^2 \cdot 7$, e trocamos esta congrência por

$$\begin{aligned} x &\equiv 3 \pmod{5^2} \\ x &\equiv 3 \pmod{7} \end{aligned}$$

O sistema resultante é equivalente ao original já que, sendo p, q primos, $x \equiv a_i \pmod{p^e}$, $x \equiv a_i \pmod{q^f}$ implica que $x \equiv a_i \pmod{p^e q^f}$.

Eliminamos os módulos compostos. No entanto, o sistema resultante pode ainda ter módulos que não são co-primos entre si, porque o mesmo primo pode estar presente na fatoração de mais de um m_i. Por exemplo, o sistema

$$\begin{aligned} x &\equiv 8 \pmod{175} \\ x &\equiv 3 \pmod{5} \end{aligned}$$

seria transformado em

$$\begin{aligned} x &\equiv 8 \pmod{25} \\ x &\equiv 8 \pmod{7} \\ x &\equiv 3 \pmod{5}, \end{aligned} \tag{6.3}$$

e temos os módulos $25 = 5^2$ e 5 no mesmo sistema.

Suponha agora que

$$\begin{aligned} m_i &= \cdots p^N \cdots, \\ m_j &= \cdots p^n \cdots, \\ N &> n. \end{aligned}$$

Ou seja, p^N, com expoente maior, está na fatoração de m_i; p^n, com expoente menor, está na fatoração de m_j. Por exemplo, em 6.3, $m_1 = 25 = 5^2$, e $m_3 = 5 = 5^1$ – neste caso, p^N é 5^2, e p^n é 5^1.
Então $p^n \mid \mathrm{mdc}\,(m_i, m_j)$.
Como $\mathrm{mdc}\,(m_i, m_j) \mid (a_i - a_j)$,

$$\begin{aligned} & p^n \mid \mathrm{mdc}\,(m_i, m_j) \mid (a_i - a_j) \\ & p^n \mid (a_i - a_j) \\ & a_i \equiv a_j \pmod{p^n}. \end{aligned} \tag{6.4}$$

Observamos agora que, se $N > n$,

$$\begin{aligned} x &\equiv a_i \pmod{p^N} && \\ p^N &\mid x - a_i && \text{(definição de congruência)} \\ p^n &\mid x - a_i && \text{(N>n)} \\ x &\equiv a_i \pmod{p^n} && \text{(definição de congruência)} \end{aligned}$$

e $x \equiv a_i \pmod{p^N}$ implica em $x \equiv a_i \pmod{p^n}$. Mas à luz da equação 6.4, isso implica que $x \equiv a_j \pmod{p^n}$, e concluímos que

$$x \equiv a_i \pmod{p^N}$$

implica em

$$x \equiv a_j \pmod{p^n},$$

e podemos remover, dentre as congruências de módulo potência de um mesmo primo, todas exceto a da maior potência.
O resultado é um sistema de congruências equivalente ao original, mas onde cada congruência tem como módulo uma potencia de primo, sem que haja repetição dos primos. Os módulos são, portanto, co-primos, e pelo Teorema Chinês dos Restos, podemos resolver o sistema. □

Exemplo 6.10. *Considere o sistema de congruências*

$$\begin{aligned} x &\equiv 31 \pmod{72} \\ x &\equiv 15 \pmod{20} \\ x &\equiv 13 \pmod{42} \end{aligned}$$

Verificamos que $\mathrm{mdc}\,(m_i, m_j) \mid (a_i - a_j)$*:*

$$\begin{aligned}
&\mathrm{mdc}\,(72, 20) = 4 \mid 16 = 31 - 15\\
&\mathrm{mdc}\,(72, 42) = 6 \mid 18 = 31 - 13\\
&\mathrm{mdc}\,(20, 42) = 2 \mid 2 = 15 - 13
\end{aligned}$$

Substituímos as congruências por outras, com módulos potencia de primo.

$$\begin{aligned}
72 &= 2^3 \cdot 3^2\\
20 &= 2^2 \cdot 5\\
42 &= 2^2 \cdot 3 \cdot 7
\end{aligned}$$

portanto o primeiro sistema equivalente é

$$\begin{aligned}
x &\equiv 31 \pmod{2^3}\\
x &\equiv 31 \pmod{3^2}\\
x &\equiv 15 \pmod{2^2}\\
x &\equiv 15 \pmod{5}\\
x &\equiv 13 \pmod{2}\\
x &\equiv 13 \pmod{3}\\
x &\equiv 13 \pmod{7}
\end{aligned}$$

Eliminamos $x \equiv 15 \pmod{2^2}$*,* $x \equiv 13 \pmod{2}$ *e* $x \equiv 13 \pmod{3}$*, e obtemos*

$$\begin{aligned}
x &\equiv 31 \pmod{2^3}\\
x &\equiv 31 \pmod{3^2}\\
x &\equiv 15 \pmod{5}\\
x &\equiv 13 \pmod{7}.
\end{aligned}$$

Agora os módulos são co-primos, e podemo usar o Teorema Chinês dos restos. Obtemos $x = 895$*, que será único módulo* $\mathrm{mmc}(72, 20, 42) = 2520$*. É trivial verificar o resultado:*

$$\begin{aligned}
895 &\equiv 31 \pmod{72}\\
895 &\equiv 15 \pmod{20}\\
895 &\equiv 13 \pmod{42}.
\end{aligned}$$

◀

O Lemma 6.6 determina que a solução do sistema, quando existe, é única módulo MMC dos módulos. Sua demonstração é pedida no Exercício 159.

Lema 6.6. *Se os módulos em um sistema de congruências como o descrito no Lema 6.5 não são co-primos e existe uma solução, ela é única módulo*

$\mathrm{mmc}(m_1, m_2, \ldots, m_k)$.

Os lemas anteriores tem como consequência a validade do Teorema a seguir.

Teorema 6.17. *Sejam* $1 < m_1, m_2, \ldots, m_k \in \mathbb{N}$ *e* $d = \mathrm{mdc}\,(m_1, m_2, \ldots, m_k)$. *Então um sistema de congruências*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_k \pmod{m_k}. \end{aligned}$$

tem solução se e somente se $d \mid (a_i - a_j)$ *para todos* $i \neq j$*, e a solução é única módulo* $\mathrm{mmc}(m_1, m_2, \ldots, m_k)$.

6.5 O Teorema Chinês dos Restos, novamente

O Teorema Chinês dos Restos tinha como contexto original a contagem módulo algum inteiro, e sua expressão moderna, na forma de congruências, foi dada por Gauss.

A partir da metade do Século XIX houve uma tendência à abstração, e o conceito de congruência mostrou-se insuficiente para expressar o que matemáticos pensavam (nasceu nesse período a Álgebra em sua forma abstrata, moderna), e novas idéias foram sendo introduzidas. Em particular, anéis e ideais. Pessoas centrais neste processo foram Leopold Kronecker[27], Richard Dedekind[28] e Emmy Noether[29]. Em algum momento entre a metade do Século XIX e o início do século XX, o Teorema Chinês dos Restos teve seu enunciado trocado por uma forma mais abstrata e abrangente, envolvendo anéis e ideais. Esta Seção traz uma versão ligeiramente simplificada da versão moderna[30].

Apresentamos novamente o Teorema Chinês dos Restos, mas desta vez usando isomorfismo entre anéis, e restringindo ao caso particular em que os anéis são $\mathbb{Z}_n$ e $\mathbb{Z}_m$.

[27] Leopold Kronecker (1823-1891), Alemão.
[28] Richard Dedekind (1831-1916), Alemão.
[29] Emmy Noether (1882-1935), Alemã.
[30] Uma versão do enunciado moderno usual é "Em um anel comutativo unitário R com ideais $I_1, \ldots, I_n$, mutuamente coprimos aos pares (ou seja, se $i \neq j$ então $I_i + I_j = R$), o mapa natural $R \to R/I_1 \times \cdots \times I_i$ é sobrejetor com núcleo $I_1 \cap \cdots \cap I_n$, e portanto induz um isomorfismo $R/(I_1 \cap \cdots \cap I_n) \cong \prod R/I_j$". Este texto não define ideal de um anel, e o Teorema pode ser enunciado sem usar explicitamente o conceito, por isso a simplificação.

Seja $n = ab$, com $\mathrm{mdc}\,(a, b) = 1$, e considere os anéis

$$\begin{aligned}\mathbb{Z}_n &= \{0, 1, 2, \ldots, n-1\},\\ \mathbb{Z}_a &= \{0, 1, 2, \ldots, a-1\},\\ \mathbb{Z}_b &= \{0, 1, 2, \ldots, b-1\},\end{aligned}$$

onde as operações são a soma e multiplicação módulo n, módulo a e módulo b.
Observe que o produto cartesiano

$$\begin{aligned}\mathbb{Z}_a \times \mathbb{Z}_b &= \{(x, y) \mid x \in \mathbb{Z}_a, y \in \mathbb{Z}_b\}\\ &= \{(0,0), (0,1), \ldots, (a-1, b-1)\}\end{aligned}$$

também é anel (as operações de soma e multiplicação módulo a e módulo b são realizadas separadamente nos dois elementos dos pares ordenados). Evidentemente,

$$|\mathbb{Z}_n| = |\mathbb{Z}_a|\,|\mathbb{Z}_b|.$$

Definimos agora uma função $f : \mathbb{Z}_n \to \mathbb{Z}_a \times \mathbb{Z}_b$, tal que

$$f(x) = \Big(x \pmod a,\ \ x \pmod b\Big). \tag{6.5}$$

É comum autores apresentarem esta função sem explicitar os módulos, "$f(x) = (x, x)$". Como o contradomínio é $\mathbb{Z}_a \times \mathbb{Z}_b$, entende-se que em (x, x) o primeiro x é tomado módulo a e o segundo, módulo b. Para evitar a confusão visual da notação de módulo e também evitar a ambiguidade, denotaremos por $[x]_z$ a classe de equivalência $x \pmod z$, e portanto

$$f(x) = \left([x]_a,\ [x]_b\right).$$

Enunciamos uma nova versão do Teorema Chinês dos Restos. Este enunciado, em um primeiro exame, não parece ter relação com o Teorema Chinês dos Restos enunciado anteriormente (Teorema 6.16) – mas a relação ficará clara adiante.

Teorema 6.18 (Chinês dos Restos)**.** *A função* f *(definida na equação 6.5) dada por*

$$\begin{aligned}f &: \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n\\ f(x) &= (x, x),\end{aligned}$$

com $\mathrm{mdc}\,(m, n) = 1$*, é bijetora.*

Demonstração. Como o domínio e contra-domínio são finitos e tem a mesma cardinalidade, se f for injetora, ela será também bijetora, necessariamente. Verificamos portanto que f é injetora.

Suponha, por absurdo, que f não é injetora: então existem inteiros x_1, x_2 tais que

$$[x_1]_n \neq [x_2]_n,$$
$$f([x_1]_n) = ([x]_a, [x]_b), \tag{6.6}$$
$$f([x_2]_n) = ([x]_a, [x]_b). \tag{6.7}$$

Mas destas equações, olhando apenas para a primeira parte dos pares ordenados, vemos que

$$\text{de } 6.6, \quad x_1 \equiv x \pmod{a}$$
$$\text{de } 6.7, \quad x_2 \equiv x \pmod{a}$$

Disso temos que

$$x_1 \equiv x_2 \pmod{a}.$$

Da mesma forma, se olharmos o lado direito dos pares ordenados, teremos

$$x_1 \equiv x_2 \pmod{b}.$$

Mas se x_1 e x_2 são congruentes nos dois módulos, então serão congruentes módulo $ab = n$. Chegamos à contradição que havíamos previsto, e terminamos a demonstração. □

Um exemplo simples ilustra claramente o que diz o Teorema 6.18.

Sejam $a = 3, b = 4$, e $n = ab = 12$. A tabela a seguir mostra a função $f(x)$, que é claramente bijetora.

$[x]_{12}$	$([x]_3, [x]_4)$	$[x]_{12}$	$([x]_3, [x]_4)$
0	(0, 0)	6	(0, 2)
1	(1, 1)	7	(1, 3)
2	(2, 2)	8	(2, 0)
3	(0, 3)	9	(0, 1)
4	(1, 0)	10	(1, 2)
5	(2, 1)	11	(2, 3)

A conexão deste Teorema com o Teorema Chinês onde apresentamos um sistema de congruências fica clara com o seguinte exemplo.

Exemplo 6.11. *Sejam* $a = 10$ *e* $b = 17$*, com* $n = ab = 170$*. Como* f *é bijeção, existe algum* x *tal que* $f(x) = (5, 12)$*; queremos determiná-lo. Mas isto é o*

mesmo que buscar a solução para

$$\begin{aligned} x &\equiv 5 \pmod{10} \\ x &\equiv 12 \pmod{17} \end{aligned}$$

Considere a equação

$$17s + 10t = 1.$$

Obtemos os coeficientes de Bézout, $s = 3, t = -5$*:*

$$3(17) - 5(10) = 1.$$

Agora multiplicamos, e chegamos a

$$51 - 50 = 1.$$

Observamos que

$$\begin{aligned} 51 &\equiv 1 \pmod{10} \\ 51 &\equiv 0 \pmod{17} \\ -50 &\equiv 0 \pmod{10} \\ -50 &\equiv 1 \pmod{17} \end{aligned}$$

Temos dois números que são congruentes a zero e um nos dois módulos, de forma que podemos escrever

$$\begin{aligned} [1]_{10}(5) + [0]_{10}(12) &\equiv 5 \pmod{10} \\ [0]_{17}(5) + [1]_{17}(12) &\equiv 12 \pmod{17} \end{aligned}$$

Ou seja,

$$\begin{aligned} (51)(5) + (-50)(12) &\equiv 5 \pmod{10} \\ (51)(5) + (-50)(12) &\equiv 12 \pmod{17} \end{aligned}$$

Não é coincidência os lados esquerdos das congruências serem idênticos: nos os construímos assim. Agora, uma vez que

$$51(5) + (-50)12 = -345 \equiv 165 \pmod{170},$$

percebemos que

$$\begin{aligned} 165 &\equiv 5 \pmod{10} \\ 165 &\equiv 12 \pmod{17} \end{aligned}$$

que é o que procurávamos. ◄

Nesta Seção *usamos* isomorfismos entre anéis para obter um resultado equivalente ao Teorema Chinês dos Restos, mas ainda o aplicamos somente em $\mathbb{Z}_n$. O Teorema pode ser também generalizado para que seja *aplicado em* anéis arbitrários – tópico fora do escopo deste texto.
Já tratamos de como resolver um sistema com duas congruências. Não é difícil adaptar o segundo enunciado do Teorema Chinês dos Restos (Teorema 6.18) para um número arbitrário de congruências.

6.6 Congruências lineares em n variáveis

Tratamos anteriormente de congruências lineares em uma única variável. Queremos também poder resolver congruências lineares em várias variáveis,

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n \equiv b \pmod{m}.$$

Da mesma forma que para congruências lineares em uma variável, é necessário que $\operatorname{mdc}(a_1, a_2, \ldots, a_n, m) \mid b$ para que haja solução.
Primeiro observamos que esta congruência é equivalente à equação Diofantina

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n - b = km$$

onde as incógnitas são os a_i e k.
Para maior clareza, iniciamos com um exemplo em três variáveis,

$$a_1x_1 + a_2x_2 + a_3x_3 = s \tag{6.8}$$

Sabemos que, fixados $a_1, a_2 \in \mathbb{Z}$ os valores possíveis para $a_1x + a_2y$ são múltiplos de $\operatorname{mdc}(a_1, a_2)$. Assim, a equação 6.8 pode ser reescrita

$$\operatorname{mdc}(a_1, a_2)\, r + a_3x_3 = s,$$

com duas incógnitas (r e x_3). Agora podemos resolvê-la obtendo os coeficientes de Bézout. Encontrados r e x_3, resolvemos a equação

$$a_1x_1 + a_2x_2 = \operatorname{mdc}(a_1, a_2)\, r,$$

que evidentemente sempre terá solução, já que $\operatorname{mdc}(a_1, a_2)$ divide o lado direito.
É possível adaptar este método para qualquer número de variáveis, eliminando uma de cada vez, desde que $\operatorname{mdc}(a_1, a_2, \ldots, a_n) \mid s$. O Exercício 161 pede o desenvolvimento deste algoritmo.
É possível também determinar o número de soluções da congruência; é disso que trata o Teorema 6.19. O Exercício 162 pede a demonstração deste Teorema.

Teorema 6.19. *Sejam* $a_1, a_2, \ldots, a_n, m$ *inteiros positivos, e seja também* $d = \mathrm{mdc}(a_1, a_2, \ldots, a_n, m)$ *e* $b \in \mathbb{Z}$*. Então a congruência*

$$a_1x_1 + \cdots + a_nx_n \equiv b \pmod{m}$$

tem dm^{n-1} *soluções incongruentes módulo* m*, quando* $d \mid b$*. Se* $d \nmid b$*, não há soluções.*

6.7 Congruências polinomiais de qualquer grau

É natural que tentemos obter também soluções para congruências não lineares. Nesta seção tratamos das congruências polinomiais em uma variável.

Definição 6.3 (congruência polinomial)**.** *Uma congruência da forma*

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x_1 + a_0 \equiv 0 \pmod{m},$$

com $a_i \in \mathbb{Z}$*, com pelo menos um* $a_i \not\equiv 0 \pmod{m}$*, é uma* ***congruência polinomial****. O* ***grau*** *da congruência é o maior* j *tal que* $a_j \not\equiv 0 \pmod{m}$*.* ◀

É importante observar que o grau de uma congruência não é necessariamente igual ao do polinômio usado para descrevê-la. Por exemplo, o grau do polinômio $10x^2+3x-2$ é dois; mas o grau da congruência $10x^2+3x-2 \equiv 0 \pmod 5$ é um, e não dois, porque $10 \equiv 0 \pmod 5$. Esta congruência na verdade é equivalente a $0x^2 + 3x - 2 \equiv 0 \pmod 5$, ou seja, $3x - 2 \equiv 0 \pmod 5$, já que $10x^2$ sempre será congruente a zero módulo 5, e pode ser ignorado.

Teorema 6.20. *Se* a *é solução para uma congruência* $f(x) \equiv 0 \pmod{m}$ *e* $d \mid m$*, então* a *também é solução para* $f(x) \equiv 0 \pmod{d}$*.*

Demonstração. Segue imediatamente do Teorema 6.5 (parte ii)[31]. □

O fato de toda solução módulo d ser também solução módulo m, múltiplo de d, não implica que não haja *mais* soluções módulo m. O Teorema 6.21 mostra que pode, realmente, haver mais soluções. Na demonstração dada usamos o Teorema Chinês dos Restos, na segunda forma, para contagem, ao invés de para obtenção das soluções.

Teorema 6.21. *Seja* $f(x)$ *um polinômio com coeficientes inteiros, e* m *um inteiro positivo. Denote por* $N(m)$ *a quantidade de soluções da congruência* $f(x) \equiv 0 \pmod{m}$*. Então, se* $m = m_1m_2$*, com* m_1 *e* m_2 *co-primos,* $N(m) = N(m_1)N(m_2)$*.*

[31] **Teorema 6.5:** Para todos $a, b, c, d \in \mathbb{Z}$ e $1 < m \in \mathbb{Z}$,

(i) se $a \equiv b \pmod{m}$, então $ac \equiv bc \pmod{mc}$;

(ii) se $a \equiv b \pmod{m}$, e $d \mid m$, então $a \equiv b \pmod{d}$.

Demonstração. Se x é solução para $f(x) \equiv 0 \pmod{m}$, pelo Teorema 6.20 x também é solução para $f(x) \equiv 0 \pmod{m_1}$ e para $f(x) \equiv 0 \pmod{m_2}$. Pelo Teorema Chinês dos restos, como $\operatorname{mdc}(m_1, m_2) = 1$, então $g(x) = ([x]_{m_1}, [x]_{m_2})$ é bijeção entre $\mathbb{Z}_m$ e $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$. Assim, para cada solução módulo m temos um par (x_1, x_2), com $x_1 \in \mathbb{Z}_{m_1}$ e $x_2 \in \mathbb{Z}_{m_2}$. O fato de g ser bijeção nos garante que o número de soluções módulo m é $N(m_1)N(m_2)$. □

É possível obter as soluções de uma congruência polinomial módulo m fatorando m e obtendo as soluções módulo p^k, para cada potência de primo na fatoração[32].
Voltamos a atenção portanto para congruências polinomiais da forma $f(x) \equiv 0 \pmod{p^a}$, com p primo.
Será interessante se pudermos reduzir o problema de obter solução para uma congruência módulo p^a a outra, módulo p^b, com $b < a$.
Procuramos as soluções de uma congruência módulo p^a. Para qualquer $b < a$, como $p^b \mid p^a$, o Teorema 6.20 nos garante que as soluções módulo p^b também são soluções módulo p^a. Obteremos agora um método para, a partir de soluções módulo p^b, chegar a soluções módulo p^a – o Lema de Hensel, demonstrado em 1904 por Kurt Hensel[33][34].

Lema 6.7 (de Hensel)**.** *Seja $f(x)$ um polinômio com coeficientes inteiros. Se $x \in \mathbb{Z}$, $f(x) \equiv 0 \pmod{p^b}$ e $f'(x) \not\equiv 0 \pmod{p}$, então existe um único t inteiro positivo tal que $f(x + tp^b) \equiv 0 \pmod{p^{b+1}}$.*

Quando $f'(x) \equiv 0 \pmod{p}$, a solução é *singular*; de outra forma, é *não singular*.
O Lema de Hensel é semelhante ao método de Newton – o que ficará claro em sua demonstração.

[32] O que não significa que seja um método prático. Para m grande, não são conhecidos algoritmos eficientes para fatoração.

[33] Kurt Hensel (1861-1941), Alemão.

[34] **Hensel**, Kurt. Neue Grundlagen der Arithmetik. **Journal für die reine und angewandte Mathematik**, v. 127, p. 51–84, 1904.

O título é "Novos Fundamentos da Aritmética", porque é onde Hensel introduziu o conceito de números p-ádicos. O lema que apresentamos aqui é uma versão diferente do original, que versava sobre polinômios com coeficientes p-ádicos. Uma breve comentário histórico é dado por David Brink (na introdução do artigo).

Brink, David. New light on Hensel's lemma. **Expositiones Mathematicae**, v. 24, n. 4, p. 291–306, 2006.

Brink também comenta que

> *Desde então, muitas variações e generalizações do resultado de Hensel foram encontradas, algumas tendo somente leve semelhança com o original. Confusamente, todos esses teoremas são conhecidos hoje como "Lema de Hensel".*
>
> *Since then, many variations and generalisations of Hensel's result have been found, some of which bear only little resemblance to the original. Confusingly, all these theorems are known today as "Hensel's lemma".*

Demonstração. Suponha que $f(x_j) \equiv 0 \pmod{p^j}$. Escrevemos a expansão de Taylor de $f(x + tp^j)$:

$$f(x + tp^j) = f(x) + tp^j f'(x) + \frac{(tp^j)^2 f''(x)}{2!} + \cdots + \frac{(tp^b)^n f^{(n)}(x)}{n!}.$$

Aogra, cada termo $a_j x^j$ no polinômio $f(x)$ contribui em cada $f^{(k)}(x)/k!$ com o termo

$$\frac{j(j-1)\cdots(j-k+1)}{k!} c_j x^{j-k} = \binom{j}{k} c_j x^{j-k}.$$

Isto significa que todos os $f^{(k)}(x)/k!$ são inteiros.
Como estamos trabalhando módulo p^{j+1}, todos os termos exceto os dois primeiros são nulos (porque todos tem p^{j+1} na fatoração). Logo,

$$f(x + tp^j) \equiv f(x) + tp^j f'(x) \pmod{p^{j+1}}$$

e podemos determinar t tal que

$$f(x) + tp^j f'(x) \equiv 0 \pmod{p^{j+1}}.$$

Mas $p^j \mid f(x)$, então temos

$$tf'(x) \equiv -\frac{f(x)}{p^j} \pmod{p}.$$

Se $\operatorname{mdc}(f'(x), p) = 1$, multiplicamos a congruência pelo inverso de $f'(x)$, obtendo

$$t \equiv -\left[f'(x)\right]^{-1} \frac{f(x)}{p^j} \pmod{p}.$$

Assim, se a_j é solução para $f(x) \equiv 0 \pmod{p^j}$, então uma solução módulo p^{j+1} é

$$\begin{aligned} a_{j+1} &= a_j + tp^j \\ &= a_j + \left(-\left[f'(a_j)\right]^{-1} \frac{f(a_j)}{p^j}\right) p^j \\ &= a_j - \left[f'(a_j)\right]^{-1} f(a_j). \end{aligned}$$

□

A última igualdade na demonstração é exatamente a que descreve o método de Newton-Raphson[35] para aproximação de zeros de funções reais. O Lema

[35] O método foi desenvolvido por Joseph Raphson e publicado no tratado "Analysis Aequationum Universalis" entre 1690 e 1702.

Raphson, Joseph. **Analysis Aequationum Universalis**. [*S. l.: s. n.*], 1702. Original em Latim disponível em https://archive.org/details/bim_eighteenth-century_analysis-quationum-univ_raphson-joseph_1702.

de Hensel é, exatamente, a aplicação desse método, mas em versão p-ádica. O exercício 163 pede a contagem do número de soluções (o enunciado do Corolário 6.1).

Corolário 6.1. *O número de soluções será zero se* $p|f'(x)$ *mas* $p \nmid \frac{f(x)}{p^b}$*; um se* $p \nmid f'(x)$*, e* p *se* p *divide tanto* $f'(x)$ *como* $\frac{f(x)}{p^b}$*.*

Exemplo 6.12. *Tentaremos identificar as soluções da congruência*

$$x^3 + 2x^2 - x - 2 \equiv 0 \pmod{27}.$$

Temos os polinômios

$$\begin{aligned} f(x) &= x^3 + 2x^2 - x - 2 \\ f'(x) &= 3x^2 + 4x - 1. \end{aligned}$$

Como $27 = 3^3$*, tentaremos inicialmente encontrar soluções para*

$$f(x) \pmod{3}$$

Uma vez que temos um primo suficientemente pequeno, podemos tentar as únicas possibilidades de solução, $0, 1, 2$*.*

$$\begin{aligned} f(0) = -2 &\equiv 1 \pmod{3} \\ f(1) = 0 &\equiv 0 \pmod{3} \\ f(2) = 12 &\equiv 0 \pmod{3} \end{aligned}$$

As soluções módulo três são 1 *e* 2*. Verificamos as derivadas de* f *nesses valores.*

$$\begin{aligned} f'(1) = 6 &\equiv 0 \pmod{3} \\ f'(2) = 19 &\equiv 1 \pmod{3} \end{aligned}$$

Também por Isaac Newton, em 1671, mas o texto de Newton só foi publicado décadas depois, em 1736, no tratado "The Method of Fluxions" (o que hoje chamamos de "derivada" era chamado de "fluxion" por Newton – um "fluxion" é a taxa de variação de um "fluente"):

Newton, Isaac. **The Method of Fluxions and Infinite Series: With Its Application to the Geometry of Curve-lines**. [*S. l.: s. n.*], 1736. "By Sir Isaac Newton, Translated from the Author's Latin Original Not Yet Made Publick. To which is Subjoin'd, a Perpetual Comment Upon the Whole Work, By John Colson, Sir Isaac Newton. Henry Woodfall; and sold by John Nourse". Tradução do original para o Inglês em `https://archive.org/details/methodoffluxions00newt`. O manuscrito original em Latim, com a caligrafia de Newton, "De Methodis Serierum et Fluxionum", pode ser lido em `https://cudl.lib.cam.ac.uk/view/MS-ADD-03960/100`.

O método, da forma como conhecemos hoje, é mais parecido com a apresentação de Raphson do que a de Newton (que era mais complicada).

O Lema de Hensel não nos permite usar a solução 1*, porque* $f'(1) \equiv 0 \pmod 3$*. Usaremos* $x_1 = 2$*. O inverso de* $f'(2)$ *é*

$$\begin{aligned}\left[f'(2)\right]^{-1} &\equiv (1)^{-1} \pmod 3 \\ &\equiv 1 \pmod 3.\end{aligned}$$

A solução módulo 3^2 *é*

$$\begin{aligned}x_2 &= x_1 - \left[f'(2)\right]^{-1} f(2) \\ &= 2 - (1)(12) \\ &= -10 \\ &\equiv 8 \pmod 9\end{aligned}$$

Verificamos:

$$f(8) = 630 \equiv 0 \pmod 9.$$

A solução módulo 3^3 *é*

$$\begin{aligned}x_3 &= x_2 - \left[f'(2)\right]^{-1} f(8) \\ &= 8 - (1)(630) \\ &= -622 \\ &\equiv 26 \pmod{27}\end{aligned}$$

Finalmente,

$$f(26) = 18900 \equiv 0 \pmod{27}.$$

Note que $p \nmid f'(x)$ *– ou seja,* $3 \nmid 19$*, e pelo Corolário 6.1, há uma só solução.* ◀

O Lema de Hensel trata apenas de soluções não-singulares. É possível, em algumas situações, elevar uma solução singular módulo p^j para j^{j+1}, conforme o enunciado do Teorema 6.22. A demonstração (na verdade muito simples) é pedida no exercício 164.

Teorema 6.22. *Seja* x_j *uma solução para* $f(x) \equiv 0 \pmod{p^j}$*. Se* $f(x_j) \equiv 0 \pmod{p^{j+1}}$ *então* $f(a + kp^j) \equiv 0 \pmod{p^{j+1}}$*, para todo inteiro* k*.*

Exemplo 6.13. *Tentaremos identificar as soluções da congruência*

$$x^3 - 100x \equiv 0 \pmod{25}.$$

Temos os polinômios

$$\begin{aligned}f(x) &= x^3 - 100x \\ f'(x) &= 3x^2 - 100.\end{aligned}$$

Como $25 = 5^2$*, tentaremos inicialmente encontrar soluções para*

$$x^3 - 100x^2 \pmod 5$$

Uma vez que temos um primo suficientemente pequeno, podemos tentar as únicas possibilidades de solução, $0, 1, 2, 3, 4$*.*

$$\begin{aligned} f(0) = \quad 0 &\equiv 0 \pmod 5 \\ f(1) = -99 &\equiv 1 \pmod 5 \\ f(2) = -192 &\equiv 3 \pmod 5 \\ f(3) = -273 &\equiv 2 \pmod 5 \\ f(4) = -336 &\equiv 4 \pmod 5 \end{aligned}$$

A única solução módulo cinco é $x_1 = 0$*. Verificamos as derivadas de* f *em zero.*

$$f'(0) = -100 \equiv 0 \pmod 5$$

O Lema de Hensel não nos permite usar a solução zero, porque $f'(0) \equiv 0 \pmod 5$*.*
Agora, mesmo x_1 *sendo singular, temos* $f(x_1) \equiv 0 \pmod{5^2}$*. Logo, pelo Teorema 6.22,*

$$f(x_1 + 5k) \equiv 0 \pmod{5^2},$$

e temos as soluções $0, 5, 10, 15, 20$*:*

$$\begin{aligned} f(0) = 0 &\equiv 0 \pmod{25} \\ f(5) = -375 &\equiv 0 \pmod{25} \\ f(10) = 0 &\equiv 0 \pmod{25} \\ f(15) = 1875 &\equiv 0 \pmod{25} \\ f(20) = 6000 &\equiv 0 \pmod{25} \end{aligned}$$

São cinco soluções módulo 25*, como queríamos.* ◀

Definição 6.4 (polinômios equivalentes, congruentes e reduzidos módulo p)**.** *Sejam* p *um primo e* f, g *dois polinômios.*

i) Se para todos os possíveis valores $x_1, x_2, \ldots, x_n \in \mathbb{Z}_p$*,* $f(x_1, x_2, \ldots, x_n) \equiv g(x_1, x_2, \ldots, x_n)$*, então* f *é* ***equivalente*** *a* g*.*

ii) Se para todos os coeficientes a_i*,* b_i*, for verdade que* $a_i \equiv b_i \pmod p$*, então* f *é* ***congruente*** *a* g

iii) Se o grau de f *é menor que* p*,* f *é* ***reduzido*** *módulo* p*. módulo* p*.*

◀

O Teorema 6.23, de Lagrange, é o semelhante em aritmética modular ao Teorema Fundamental da Álgebra.

Teorema 6.23 (de Lagrange)**.** *Seja* $f(x)$ *um polinômio de grau* n *com coeficientes integrais, e* p *um primo que* não *divide o coeficiente líder de* $f(x)$*. Então a congruência* $f(x) \equiv 0 \pmod{p}$ *tem no máximo* n *soluções incongruentes módulo* p*.*

Demonstração. Procedemos por indução no grau do polinômio $f(x)$. A base de indução é com graus zero e um.
Quando $f(x)$ tem grau zero, a congruência é $a_0 \equiv 0 \pmod{p}$, e há zero soluções.
Quando $f(x)$ tem grau um, a congruência é $a_1x + a_0 \equiv 0 \pmod{p}$. Como sempre há inversos módulo primo, a_1 tem inverso, e a congruência tem exatamente uma solução $x \equiv -a_0(a_1)^{-1} \pmod{p}$.
Presumimos que o enunciado vale para polinômios de grau menor que k, com $k \geq 2$. Suponha que uma congruência $f(x) \equiv 0 \pmod{p}$ de grau k tenha mais que k soluções. Seja a_kx^k o primeiro termo de $f(x)$, e $y_1, y_2, \ldots, y_{k+1}$ soluções, *todas incongruentes módulo* p, desta congruência. Seja

$$g(x) = f(x) - a_k(x - y_1)(x - y_2)\cdots(x - y_{k+1}).$$

Como os y_i são soluções, $(x-y_1)\cdots(x-y_n)$ será congruente a $f(x)$ módulo p. Mas $f(x) \equiv 0 \pmod{p}$, e

$$\begin{aligned} g(y_i) &\equiv f(y_i) - a_k(y_i - y_1)(y_i - y_2)\cdots(y_i - y_i)\cdots(y_i - y_k) \\ &\equiv 0 \pmod{p}, \end{aligned}$$

para todo y_i. Mas $g(x)$ tem grau menor que k (o termo líder de $f(x)$ é cancelado por a_kx^k em $g(x)$). Isto significa que temos uma congruência de grau menor que k, com mais que k soluções. Como p não divide o termo líder de $f(x)$, o grau de $f(x)$ é $k+1$. Pela hipótese de indução, só nos resta supor que, para todo x inteiro,

$$g(x) \equiv 0 \pmod{p}.$$

Ou seja, $g(x)$ é identicamente zero.
Tomamos então y_{k+1}.

$$\begin{aligned} g(y_{k+1}) &\equiv f(y_{k+1}) - a_0(y_{k+1} - y_1)(y_{k+1} - y_2)\cdots(y_{k+1} - y_i)\cdots(y_{k+1} - y_k) \\ &\equiv -a_0(y_{k+1} - y_1)(y_{k+1} - y_2)\cdots(y_{k+1} - y_i)\cdots(y_{k+1} - y_k) \quad (6.9) \\ &\equiv 0 \pmod{p} \end{aligned}$$

Mas Isto não é possível, porque $p \nmid a_0$, e p também não divide nenhum dos fatores no lado direito da congruência 6.9, porque são diferenças entre números incongruentes módulo p. Chegamos a uma contradição, e a demonstração está pronta. □

Corolário 6.2. *Se* $a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}$ *tem mais que* n *soluções, então para todo coeficiente* a_i, $p \mid a_i$, *(o polinômio no lado esquerdo é congruente ao polinômio zero módulo* p*).*

Os Lemas 6.8, 6.9 e 6.10 afirmam que sempre é possível trabalhar com polinômios reduzidos. A demonstração do Lema 6.9 é pedida no Exercício 165.

Lema 6.8. *Se* f *e* g *são polinômios módulo* p*, e* $f \sim g$*, então* $f \equiv g$*.*

Lema 6.9. *Dados um polinômio* f *e um primo* p*, existe outro polinômio* g *tal que* g *é reduzido módulo* p

Lema 6.10. *Se* f *e* g *são reduzidos módulo* p*, e* $f \equiv g$*, então* $f \sim g$*.*

Teorema 6.24 (de Chevalley)**.** *Seja* f *um polinômio em* n *variáveis, com grau* $h < n$*, e seja*

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{p}$$

uma congruência.

i) Se a congruência tem solução, então ela tem pelo menos duas soluções.

ii) Se f *é homogêneo, então a congruência tem alguma solução diferente de* $(0, \ldots, 0)$.

A forma como enunciamos este Teorema foi demonstrada por Chevalley[36] em 1935. Warning[37] mostrou que no caso (i), além do que é afirmado no enunciado, a quantidade de soluções é divisível por p[38]. A demonstração a seguir é praticamente a mesma dada por H. E. Rose (Rose, 1988).

[36] Claude Chevalley (1909-1984), Francês; membro fundador do grupo Bourbaki.

[37] Este é EWALD WARNING, Alemão, Século XX. Não deve ser confundido com EDWARD WARING, Inglês (1736-1798), orientador e amigo de John Wilson (a nota de rodapé 4 na página 125 trata de Waring, Wilson, e o chamado "Teorema de Wilson".)

[38] Quase isso. Teoremas tem seus enunciados simplificados para exposição didática a iniciantes. No original, Chevalley reproduziu o enunciado que havia sido proposto por Emil Artin:

> *Se* k *é um corpo algebricamente fechado e* x *um elemento transcendental com respeito a* k*, uma equação da forma*
>
> $$F(y_1, y_2, \ldots, y_n) = 0$$
>
> *onde* F *é um polinômio homogêneo de grau* $< n$ *com respeito às variáveis* $y_1, y_2, \ldots, y_n$ *(coeficientes em* $k(x)$*), tem pelo menos uma solução não trivial em* $k(x)$.

O original, em francês:

> *Si* k *est un corps algébriquement fermé, et* x *un élément transcendant par*

Demonstração. Para (i): Suponha, por contradição, que $(a_1, \ldots, a_n)$ seja a *solução* para a congruência. Seja também

$$g(x_1, \ldots, x_n) = 1 - f(x_1, \ldots, x_n)^{p-1}.$$

Usando o Teorema de Fermat, $g(x_1, \ldots, x_n)$ será sempre um ou zero.

- $g(x_1, \ldots, x_n) = 1$ se $x_i \equiv a_i \pmod{p}$;
- $g(x_1, \ldots, x_n) = 0$ se pelo menos algum $x_i \not\equiv a_i \pmod{p}$.

Seja g' o polinômio equivalente a g, reduzido módulo p (que existe, pelo Lema 6.9).
Agora seja

$$g^* = \prod_{i=1}^{n} (1 - (x_i - a_1)^{p-1}).$$

Claramente, $g^* \equiv g'$. Como g^* é reduzido, então $g^* \sim g'$ (pelo Lema 6.10).

---

rapport à k*, une équation de la forme*

$$F(y_1, y_2, \ldots, y_n) = 0$$

où F *est un polynome homogène de degré* $< n$ *par rapport aux variables* $y_1, y_2, \ldots, y_n$ *à coefficients dans* $k(x)$ *posséde au moins une solution non-triviale dans* $k(x)$.

Chevalley, C. Démonstration d'une hypothèse de M. Artin. **Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg**, v. 11, p. 73–75, 1935.

O resumo do artigo de Ewald Warning começa com a seguinte afirmação:

> *No artigo anterior, o Sr. Chevalley provou que se um sistema de polinômios (com coeficientes provenientes de um corpo de Galois), cujo número de variáveis é maior que a soma dos graus dos polinômios individuais, possui uma raiz comum 0, então ele sempre possui outra raiz comum.*
> *Continuando a linha de raciocínio do Sr. Chevalley, demonstraremos a seguir que certas relações existem entre as raízes de tal sistema de polinômios, das quais se depreende, em particular, que o número de raízes é divisível pela característica do corpo de Galois. O número de raízes é, portanto,* $= 0$ *ou* $\geq$ *que a característica.*

O original, em Alemão:

> *In der vorstehenden Arbeit hat Herr CHEVALLEY bewiesen: Falls ein System con Polynomen (mit Koeffizienten aus einem Galois-Feld), dessert Variablenzahl größer als die Summe der Grade der einzelnen Polynome ist, die gemeinsame Nullstelle 0 hat, so hat es stets noch eine weitere gemeinsame Nullstelle.*
> *Durch Fortfführung des Beweisgedankens von Herrn CHEVALLEY soll im folgenden gezeigt werden, daß zwischen den Nullstellen eines solchen Systems yon Polynomen gewisse Relationen bestehen, aus denen insbesondere folgt, daß die Anzahl der Nullstellen durch die Charakteristik des Galois-Feldes teilbar ist. Die Anzahl der Nullstellen ist also entweder* $= 0$ *oder* $\geq$ *der Charakteristik.*

Warning, E. Bemerkung zur vorstehenden Arbeit von Herrn Chevalley. **Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg**, v. 11, p. 76–83, 1935.

Mas temos

$$\begin{aligned}\deg g' \leq \deg g = r(p-1),\\ \deg g^* = n(p-1).\end{aligned}$$

No entanto, $g^* \sim g'$ não podem ter graus diferentes. Chegamos à contradição, e a afirmação (i) do enunciado está demonstrada.
Para (ii): Um sistema homogêneo sempre tem a solução zero, portanto (i) (que já demonstramos) implica que deve haver alguma outra solução além do zero. □

6.8 Sequência de Fibonacci módulo m

Diversos fatos interessantes surgem quando tomamos a conhecida sequência de Fibonacci, módulo algum natural maior que dois[39].

Definição 6.5 (sequência de Fibonacci módulo m)**.** *Se $m \in \mathbb{N}$, $m > 1$, a **sequência de Fibonacci módulo** m é a sequência $u_i \pmod m$, onde u_i é o i-ésimo número de Fibonacci. Esta sequência será denotada por $u(\mathrm{mod}\, m)$.* ◀

Exemplo 6.14. *Listamos os 20 primeiros números de Fibonacci, e seus valores módulo 2, 3 e 4.*

$$\begin{aligned}(u_n) &= 1,1,2,3,5,8,13,21,34,55,89,144,233,377,\\ &\quad\ 610,987,1597,2584,4181,6765,\ldots\\ u(\mathrm{mod}\,2) &= 1,1,0,1,1,0,1,1,0,1,1,0,1,1,0,1,1,0,1,1,\ldots\\ u(\mathrm{mod}\,3) &= 1,1,2,0,2,2,1,0,1,1,2,0,2,2,1,0,1,1,2,0,\ldots\\ u(\mathrm{mod}\,4) &= 1,1,2,3,1,0,1,1,2,3,1,0,1,1,2,3,1,0,1,1,\ldots\end{aligned}$$

Interessantemente, a sequência $u(\mathrm{mod}\,2)$ parece ser periódica (o padrão $1,1,0$ se repete). Também em $u(\mathrm{mod}\,3)$, o padrão $1,1,2,0,2,2,1,0$ parece se repdroduzir, assim como em $u(\mathrm{mod}\,4)$ o padrão $1,1,2,3,1,0$ se repete. ◀

[39] A idéia de tomar a sequência de Fibonacci módulo m é de D. D. Wall, em 1960. Wall afirma que

> *O problema surgiu em conexão com um método para gerar números aleatórios, mas acabou se mostrando inesperadamente complexo, então rapidamente se tornou objeto de interesse por si mesmo.*

No original,

> *The problem arose in connection with a method for generating random numbers, but it turned out to be unexpectedly intricate, and so quickly became of interest in its own right.*

Wall, D. D. Fibonacci Series Modulo m. **The American Mathematical Monthly**, v. 67, n. 6, p. 525–532, 1960.

O Exemplo 6.14 nos motivaa questionar se as sequencias $u \pmod n$ são periódicas, e é isso que o Lema 6.11 estabelece.

Lema 6.11. *Para qualquer m, a sequência de Fibonacci módulo m é periódica.*

Demonstração. Inicialmente observamos que a sequência de Fibonacci (u_n) é definida recursivamente com dois casos base, e portanto quaisquer dois inteiros determinam toda a sequência depois deles.
Além disso, em $u \pmod m$ os elementos são restos de divisão por m, e há para cada um deles há, portanto, m possibilidades. Para cada par de elementos da sequência (que determinam o resto dela) há, portanto, m^2 possibilidades.
Como consequência, ao longo da sequência algum par necessariamente se repetirá, porque m^2 é finito. Quando esse par se repetir o período da sequência recomeçará. □

Definição 6.6. *O **período** de uma sequência de Fibonacci módulo m (também chamado de **período de Pisano para** m), denotado*[40] $k(m)$*, é o número de termos de $u \pmod m$ em cada ciclo*[41]*.* ◀

Listamos alguns dos valores de $k(m)$.

$$\begin{aligned} k(2) &= 3 & \qquad k(7) &= 16 \\ k(3) &= 8 & \qquad k(8) &= 12 \\ k(4) &= 6 & \qquad k(9) &= 24 \\ k(5) &= 20 & \qquad k(10) &= 60 \\ k(6) &= 24 \end{aligned}$$

Teorema 6.25. *Se $m > 2$, então $k(m)$ é par.*

Demonstração. O Lema 4.7 determina que $u_{(-n)} = (-1)^{n+1} u_n$. Assim, quando n é ímpar, $u_n = u_{(-n)}$. Presumimos agora que $k(m)$ é ímpar.

$$u_1 = u_{(-1)} \equiv u_{k-1} \pmod m.$$

Como $k-1$ é par, $u_{k-1} = -u_{1-k} \equiv -u_1$. Então $u_1 \equiv -u_1 \pmod m$, mas isto só é possível quando $m = 2$.
Como m deve ser 2 para valores ímpares de k, então todos os outros valores de k devem ser pares. □

O Exercício 169 pede a demonstração do Teorema 6.26.

[40] Há autores que o denotam por $\pi(m)$, mas neste texto usaremos $\pi(n)$ para denotar uma função aritmética, na Seção 8.6.

[41] Ou ainda, $k(m)$ é o período (no sentido usual, período de função) de $u \pmod m$.

Teorema 6.26. *Se* $g \mid m$*, então* $k(g) \mid k(m)$.

O Teorema 6.27 tem como consequência podermos restringir o estudo de períodos de Pisano a potências de primos, porque quando m é composto, $k(m)$ pode ser determinado a partir dos períodos das potências de primos na fatoração de m.

Teorema 6.27. *Se a fatoração de* m *é* $m = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$*, então* $k(m)$ *é o MDC dos* $k(p_i^{a_i})$*:*

$$k(m) = \operatorname{mmc}(k(p_1^{a_1}), k(p_2^{a_2}), \dots, k(p_r^{a_r}))$$

A seguir está um rascunho da demonstração. O Exercício 171 pede para completá-la.

Demonstração. (Rascunho)
O Teorema 6.27 garante que $k(p_i^{a_i}) \mid k(m)$ para todo i. Assim,

$$\operatorname{mmc}(k(p_i^{a_i})) \mid k(m). \qquad \text{(mmc de todos os } p_i^{a_i}\text{)}$$

Mas como evidentemente $k(p_i^{a_i}) \mid \operatorname{mmc}(k(p_i^{a_i}))$, temos que $u \pmod{p_i^{a_i}}$ deve repetir sequências de tamanho $\operatorname{mmc}(k(p_i^{a_i}))$. Assim $u_{\operatorname{mmc}(k(p_i^{a_i}))} \equiv u_0 \pmod{p_i^{a_i}}$ e $u_{\operatorname{mmc}(k(p_i^{a_i}))+1} = u_1 \pmod{p_i^{a_i}}$. Usando o Teorema Chinês dos restos, passamos para módulo m. □

A partir disto, a demonstração do Teorema 6.28 não é dificil (e é pedida no Exercício 170).

Teorema 6.28. $k(\operatorname{mmc}(m,s)) = \operatorname{mmc}(k(m), k(s))$.

A demonstração do Teorema 6.29 é pedida no Exercício 172. Este Teorema relaciona o período de uma sequência de Fibonacci módulo potência de primo.

Teorema 6.29. *Seja* t *o maior inteiro tal que* $k(p^t) = k(p)$*. Então* $k(p^s) = p^{s-t} k(p)$.

Exercícios

Ex. 133 — Prove que para todo $a > 0$ e todo $m > 1$, $a \equiv a \pmod{m}$.

Ex. 134 — Prove que para todo x ímpar e todo inteiro positivo n,

$$x^{2^n} \equiv 1 \pmod{2^{n+2}}$$

Ex. 135 — Prove que se p é primo, $n < p < 2n$, então

$$\binom{2n}{n} \equiv 0 \pmod{p}$$

Ex. 136 — Prove que, para todos $x, y, z \in \mathbb{N}$, se $x^2+y^2 = z^2$, com $\operatorname{mdc}(x, y, z) = 1$, então $3 \mid x$ ou $3 \mid y$ (mas não ambos!)

Ex. 137 — Existem $a, b \in \mathbb{Q}$ tais que $a^2 + b^2 = 3$?

Ex. 138 — Seja p primo. Qual é o menor inteiro positivo congruente a $(p-2)!$ módulo p?

Ex. 139 — Prove que se p é primo, $ab \equiv ac \pmod{p}$, e $p \nmid a$, então $b \equiv c \pmod{p}$.

Ex. 140 — Prove que se $0 \leq |a| < m/2$, $0 \leq |b| < m/2$ e $a \equiv b \pmod{m}$, então $a = b$.

Ex. 141 — Prove que $a^x \equiv b^x \pmod{m}$ e $a^y \equiv b^y \pmod{m}$, então

$$a^{\operatorname{mdc}(x,y)} \equiv b^{\operatorname{mdc}(x,y)} \pmod{m}.$$

Ex. 142 — Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, é verdade que $x^a \equiv x^b \pmod{m}$, para $x > 1$? E é verdade que $a^b \equiv c^d \pmod{m}$?

Ex. 143 — Demonstre o Teorema 6.13.

Ex. 144 — Resolva as equações ou explique porque não é possível fazê-lo.

(a) $4x - y = 9$

(b) $15x + 21y = 18$

(c) $23x + 15y = 5$

(d) $21x + 15y = 3$

(e) $121x - 88y = 572$

Ex. 145 — Determine para quais valores de K as equações a seguir tem solução.

(a) $15Kx - 8y = 14$

(b) $2Kx + 110y = 63$

Ex. 146 — Calcule os inversos

(a) $5^{-1} \pmod{31}$

(b) $8^{-1} \pmod{21}$

(c) $13^{-1} \pmod{42}$

Ex. 147 — Mostre uma solução inteira positiva para $30x + 18y = 132$, ou prove que não existe.

Ex. 148 — No Exemplo 6.7, se trocarmos a restrição "$x, y \geq 9$" por "$x > y$", quais valores de k podemos usar?

Ex. 149 — Há soluções para a equação diofantina $4x + 8y = 36$, se exigirmos que tanto x como y não possam ser escritos como soma de quadrados? Caso haja, quais são? Caso não haja, qual o motivo? E se exigirmos isso somente de x?

Ex. 150 — Mostre que a equação diofantina $4x + 8y = 36$ (a mesma do Exercício 149) tem infinitas soluções em que x é soma de quadrados.

Ex. 151 — Prove que se p é primo ímpar, então $p \mid 2^{p-1} + (p-1)!$.

Ex. 152 — Prove que se p é primo e $m, n \in \mathbb{Z}$, com $m, n \geq 0$, tais que $m + n = p - 1$, então

$$m!n! \equiv (-1)^{n+1} \pmod{p}$$

Ex. 153 — Seja p um primo ímpar. Determine quais inteiros n existem tais que $p \mid n2^n + 1$.

Ex. 154 — Generalize a noção de congruência para o anel $\mathbb{Z}[i]$ dos inteiros Gaussianos, e prove que todo $a + bi$, é congruente a 0 ou $+1$ módulo $(1 + i)$.

Ex. 155 — Da forma como apresentamos, o Teorema Chinês dos restos nos dá solução para sistemas onde cada equação é da forma $x \equiv a_i \pmod{m_i}$. Mostre como resolver sistemas da forma $b_i x \equiv a_i \pmod{m_i}$.

Ex. 156 — Resolva os sistemas de congruências.

(i)

$$\begin{aligned} x &\equiv 2 \pmod{5} \\ x &\equiv 3 \pmod{28} \\ x &\equiv 10 \pmod{13} \end{aligned}$$

(ii)

$$\begin{aligned} x &\equiv 1 \pmod{36} \\ x &\equiv 10 \pmod{12} \\ x &\equiv 15 \pmod{470} \end{aligned}$$

(iii)

$$\begin{aligned} x &\equiv 4 \pmod{10} \\ 4x &\equiv 5 \pmod{21} \\ 10x &\equiv 2 \pmod{11} \end{aligned}$$

(iv)

$$\begin{aligned} x &\equiv 3 \pmod{20} \\ 3x &\equiv 2 \pmod{35} \\ 2x &\equiv 1 \pmod{12} \end{aligned}$$

Ex. 157 — Em dúzias, sobra um; em dezenas, sobram três; em setes, sobram seis. Qual é o número?

Ex. 158 — Há um método geral para resolver sistemas de congruências sem usar os dois enunciados do Teorema Chinês dos Restos: encontre uma solução geral para a primeira congruência, substitua na segunda, e assim por diante. Formalize este método e use-o para resolver um dos sistemas do Exercício 156.

Ex. 159 — Demonstre o Lema 159.

Ex. 160 — Desenvolva um algoritmo que, dada uma lista de números naturais $m_1, m_2, \ldots, m_k$ e um número inteiro a_1 , gere aleatoriamente (não necessariamente de maneira equiprovável) um sistema de congruências

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

de forma que o sistema tenha solução.

Ex. 161 — Desenvolva o método para resolução de congruências lineares em várias variáveis, mencionado na seção 6.6.

Ex. 162 — Demonstre o Teorema 6.19.

Ex. 163 — Demonstre o Corolário 6.1.

Ex. 164 — Demonstre o Teorema 6.22.

Ex. 165 — Demostreo Lema 6.9.

Ex. 166 — Resolva

(a) $x^4 - x^3 - x^2 + x \equiv 0 \pmod{25}$

(b) $x^2 - 6x^2 + 8x \equiv 0 \pmod{81}$

(c) $x^3 - 8x + 20x - 16 \equiv 0 \pmod{49}$

Ex. 167 — Seja $M(x) : \mathbb{Z}_p \to \mathbb{Z}_p$ uma função que mapeia classes de resíduos. Mostre que para todo primo p existe um polinômio $f(x)$, de grau estritamente menor que p e com coeficientes integrais, tal que $f(x) \equiv M(x) \pmod{p}$ para todo $x \in \mathbb{Z}$.

Ex. 168 — Quantas sequências de k uns consecutivos há em um período de $u \bmod(n)$?

Ex. 169 — Prove o Teorema 6.26.

Ex. 170 — Prove o Teorema 6.28.

Ex. 171 — A partir do rascunho de demonstração dado no texto, prove o Teorema 6.27.

Ex. 172 — Prove o Teorema 6.29.

Capítulo 7

Sistemas de Resíduos

Sistemas de resíduos são conjuntos finitos de números módulo um inteiro. O nome "sistema" de resíduos (restos) módulo n é usado para descrever o conjunto de inteiros que podem surgir como resto de uma divisão por n. O sistema é "completo" se incluir todos os restos (e, com a operação de soma módulo n, é um grupo aditivo), ou "reduzido", se incluir apenas os coprimos com o módulo (que portanto, com a operação de multiplicação módulo n, é um grupo multiplicativo).

O conceito de resto de divisão é evidentemente muito antigo. Problemas como o proposto por Sūnzǐ e outros matemáticos[1], onde um inteiro é determinado a partir dos restos de sua divisão por diferentes módulos despertaram o interesse pelo tratamento de restos, e formam um prenúncio do estudo sistemático de congruências. Posteriormente, Leonard Euler[2] trabalhou intensamente em tópicos que resultaram no fundamento da moderna Teoria dos Números, inclusive, ainda que não destacando explicitamente o conceito de congruência, observando números agrupados em differentes classes de acordo com o resto da divisão por um inteiro. Em seguida, Johann Carl Friedrich Gauss[3] consolidou o estudo de contruências e a diferenciação de sistemas reduzidos e sistemas completos de resíduos. Nos Séculos XIX e XX, esses conceitos foram incorporados e adaptados em outros, mais abstratos: o anel de inteiros módulo n (denotado $\mathbb{Z}/n\mathbb{Z}$)[4] pode ser definido

[1] Seção 6.4, "Teorema Chinês dos Restos".

[2] Leonard Euler (1707-1783), Suíço.

[3] Johann Carl Friedrich Gauss (1777-1855), Alemão.

[4] $\mathbb{Z}$ denota o conjunto dos inteiros, ou o anel dos inteiros. $n\mathbb{Z}$ é $\{\ldots, -2n, -n, 0, n, 2n, \ldots\}$, um *ideal* deste anel. A estrutura $integers/n\mathbb{Z}$ é um conjunto de classes de equivalência, tendo representantes $\{0, 1, \ldots, n-1\}$, e dois números são considerados equivalentes nesta estrutura se $a - b \in n\mathbb{Z}$, ou $n \mid a - b$. Por exemplo,

$$5\mathbb{Z} = \{\ldots, -10, -5, 0, 5, 10, \ldots\},$$
$$\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}, \qquad \text{(representantes de classes)}$$

e a e b são equivalentes em $\mathbb{Z}/5\mathbb{Z}$ se $a - b \in 5\mathbb{Z}$: $13 \sim 28$, porque $28 - 13 = 15 \in 5\mathbb{Z}$. O

em termos de classes de resíduos; o grupo de unidades de $\mathbb{Z}/n\mathbb{Z}$ é simplesmente um sistema reduzido de resíduos com a operação de multiplicação.

7.1 Sistemas completos e reduzidos de resíduos

Se $a \equiv b \pmod{m}$, dizemos que a e b representam o mesmo **resíduo** módulo m. Por exemplo, como $25 \equiv 4 \pmod{7}$, então 4 e 25 são o mesmo resíduo módulo 7. A palavra *resíduo* significa "resto de divisão" – veja que 4 é o resto de $25 \div 7$, e também é o resto de $4 \div 7$.

Definição 7.1 (sistema completo de resíduos)**.** *Um conjunto X de inteiros é um **sistema completo de resíduos** módulo m se para cada $n \in \mathbb{Z}$, existe exeatmente um elemento em X que é congruente a n módulo m.* ◀

Ou seja, um sistema completo de resíduos módulo m identifica os possíveis restos da divisão de inteiros por m, devendo haver exatamente um elemento no sistema para cada possível resto.
O conjunto $\{0, 1, 2, \ldots, n-1\}$ é um sistema completo de resíduos módulo n, assim como $\{3, 4, 5, \ldots, n+2\}$.

Exemplo 7.1. *Mais concretamente, o conjunto $\{0, 5, 10, 15\}$ é um sistema completo de resíduos módulo quatro:*

$$\begin{aligned} 0 &\equiv 0 \pmod{4} \\ 5 &\equiv 1 \pmod{4} \\ 10 &\equiv 2 \pmod{4} \\ 15 &\equiv 3 \pmod{4}. \end{aligned}$$

Todo inteiro é congruente a $0, 1, 2$ ou 3 módulo quatro – e há exatamente um representante de cada uma destas classes de congruência no conjunto $\{0, 5, 10, 15\}$.
Em outras palavras, há exatamente um número de cada uma das formas

$$\begin{aligned} &4n + 0 \quad (0) \\ &4n + 1 \quad (5) \\ &4n + 2 \quad (10) \\ &4n + 3 \quad (15) \end{aligned}$$

◀

Definição 7.2 (sistema reduzido de resíduos)**.** *Um **sistema reduzido de resíduos** módulo m é um conjunto de inteiros co-primos com m, não congruentes entre si. Todo k inteiro co-primo com m deve ser congruente módulo m a algum elemento do conjunto.* ◀

representante da classe é 3, já que $3 \sim 13 \sim 28$, e $3 \in \{0, 1, 2, 3, 4\}$.

O conjunto $\{1, 3\}$ é um sistema reduzido de resíduos módulo quatro:

$$\begin{aligned} 1 &\equiv 1 \pmod 4 \\ 3 &\equiv 3 \pmod 4. \end{aligned}$$

Um inteiro pode ser congruente a $0, 1, 2$ ou 3 módulo quatro. No entanto, 0 e 2 não são co-primos com 4, e portanto um inteiro co-primo com m será necessariamente congruente a 1 ou 3 módulo 4.
Os elementos em um sistema reduzido de resíduos são aqueles que tem inverso (porque todos são co-primos com o módulo) – ou seja, são as *unidades* módulo m. Quando o módulo é um primo p, todos os números de 0 a $p - 1$ compõem o sistema reduzido de resíduos, e todos são unidades.
O Lema 7.1 garante que se um elemento a é parte de um sistema reduzido de resíduos, toda a sua classe de equivalência também é, porque toda ela será co-prima com o módulo.

Lema 7.1. *Se* $a \equiv b \pmod m$ *e* $\operatorname{mdc}(a, m) = 1$*, então* $\operatorname{mdc}(b, m) = 1$.

Demonstração. Se $a \equiv b \pmod m$ então

$$\begin{aligned} m \mid (a - b) \\ km &= a - b \\ a &= km + b \\ \operatorname{mdc}(a, m) &= \operatorname{mdc}(km + b, m) \\ 1 &= \operatorname{mdc}(km + b, m) \\ 1 &= \operatorname{mdc}(b, m). \end{aligned}$$

□

Para o módulo 14, o sistema reduzido de resíduos é $\{1, 3, 5, 9, 11, 13\}$. O Lema 7.1 determina que quaisquer inteiros congruentes a estes são também co-primos com 14. Podemos veriricar, como breve ilustração, que

$$\begin{aligned} 23 &\equiv 9 \pmod{14}, \\ 25 &\equiv 11 \pmod{14}, \end{aligned}$$

e tanto 23 como 23 são co-primos com 14.
É útil definir uma função para a contagem dos co-primos com n menores que ele. Essa é a função ϕ, estudada por Euler e conhecida como "função ϕ de Euler", ou "função tociente".

Definição 7.3 (funções ϕ)**.** *A função* $\phi(n)$ *dá o número de inteiros positivos* k *menores ou iguais a* n*.* ◀

Teorema 7.1. *Todo sistema reduzido de resíduos módulo* m *tem exatamente* $\phi(m)$ *elementos.*

Demonstração. Demonstramos em partes: (i) mostramos que os inteiros entre 1 e $m-1$ que são co-primos com m são todos incongruentes entre si, e portanto são um sistema reduzido de resíduos módulo m de tamaho $\phi(m)$; (ii) mostramos que um sistema reduzido de resíduos não pode ser maior que este; e (iii) mostramos que o conjunto também não pode ser menor.
(i) Suponha que $0 < a, b < m$ são co-primos com m. Como tanto a como b estão entre 1 e $m-1$, a divisão $a \div m$ deixa resto a, e a divisão $b \div m$ deixa resto b, e portanto $a \not\equiv b \pmod{m}$.
(ii) Suponha que haja um sistema reduzido de resíduos módulo m com $r > \phi(m)$ elementos $s_1, s_2, \ldots, s_r$. Cada um destes elementos é congruente módulo m a algum inteiro entre 0 e $m-1$. Sabemos que só há $\phi(m)$ inteiros a_i nesse intervalo que são co-primos com m, e também sabemos, pelo Lema 7.1, que se $s_i \equiv a_i$, e s_i é co-primo com m, então a_i deveria ser também. Mas isso significa que haveria $r > \phi(m)$ inteiros entre 0 e $m-1$ co-primos com m – uma contradição.
(iii) Um conjunto com menos de $\phi(m)$ elementos não pode ser um sistema reduzido de resíduos módulo m, porque todo inteiro co-primo com m deve ter representante de sua classe de congruência no sistema, e há pelo menos $\phi(m)$ deles, como já demonstrado na parte (i). □

É relevante que o Lema 7.1 nos permite trocar um elemento a do conjunto por qualquer inteiro b congruente a a módulo m: como são congruentes, continua havendo um representante daquela classe de congruência. Como $\mathrm{mdc}(a, n) = 1$, o Lema garante que $\mathrm{mdc}(b, m) = 1$.

Teorema 7.2. *Se* $\{r_1, r_2, \ldots, r_n\}$ *é sistema completo (ou reduzido) de resíduos módulo* m*, então para qualquer* k *co-primo com* m*, o conjunto* $\{kr_1, kr_2, \ldots, kr_n\}$ *também é.*

A demonstração segue as definições de sistemas completos e reduzidos de resíduos...

Demonstração. Primeiro (i), verificamos que ao multiplicar os elementos por k eles continuam incongruentes entre si; e depois (ii), mostramos que se $\mathrm{mdc}(r_i, m) = 1$ então $\mathrm{mdc}(kr_i, m) = 1$.
(i) se $r_i \not\equiv r_j \pmod{m}$ então $m \nmid (r_j - r_j)$, e também $m \nmid k(r_i - r_j)$, porque pelo enunciado $\mathrm{mdc}(k, m) = 1$, e m não divide k nem $(r_i - r_j)$.

Mas ao dizer "se $\mathrm{mdc}(r_i, m) = 1$", o item (ii) se aplica apenas a sistemas reduzidos, sendo irrelevante para sistemas completos de resíduos – assim uma única prova é redigida para os dois casos.

(ii) Agora, se $\mathrm{mdc}(r_i, m) = 1$, então $\mathrm{mdc}(kr_i, m)$ deve ser 1 também. Suponha que $\mathrm{mdc}(kr_i, m) = d > 1$. Isto significa que

$$d \mid kr_i$$
$$d \mid m$$

Mas como $\mathrm{mdc}(r_i, m) = 1$, d não poderia dividir tanto m como r_i, logo d deve dividir k e m – mas $\mathrm{mdc}(k, m) = 1$, e chegamos a uma contradição. d, portanto, não pode ser diferente de um. □

O sistema reduzido de resíduos módulo 14 que usamos anteriormente é $\{1, 3, 5, 9, 11, 13\}$. Multiplicamos todos por 15 (porque $\mathrm{mdc}(14, 15) = 1$), e

temos

$$\{15, 45, 75, 135, 165, 195\},$$

que também é sistema reduzido de resíduos módulo 14.
A seguir apresentamos o Teorema de Euler e o pequeno Teorema de Fermat. O segundo, na verdade, é caso particular do primeiro, portanto apresentaremos concretamente uma só demonstração. EulerEuler[5] apresentou seu trabalho, *Theoremata arithmetica nova methodo demonstrata*[6], como uma nova demonstração (e na verdade generalização) do Teorema de Fermat.

Teorema 7.3 (de Euler)**.** *Se* $\operatorname{mdc}(a, m) = 1$ *então*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Demonstração. Seja $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ um sistema reduzido de resíduos módulo m. Pelo Teorema 7.2[7], $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ também é um sistema de resíduos módulo m. Agora, como cada $ar_i \equiv r_i \pmod{m}$, então pelo Teorema 6.2[8] também vale $ar_i ar_j \equiv r_i r_j \pmod{m}$. Multiplique então todos os números ar_i:

$$\prod_{i=1}^{\phi(m)} ar_i \equiv \prod_{i=1}^{\phi(m)} r_i \pmod{m}$$

$$a^{\phi(m)} \prod_{i=1}^{\phi(m)} r_i \equiv \prod_{i=1}^{\phi(m)} r_i \pmod{m}$$

Mas como $\operatorname{mdc}(r_i, m) = 1$ para todos os r_i, podemos usar a lei do cancela-

[5] Leonard Euler (1707-1783), Suíço.

[6] O artigo é

Euler, Leonhard. Theoremata arithmetica nova methodo demonstrata. **Novi Commentarii academiae scientiarum Petropolitanae**, v. 8, p. 74–104, 1763.

O Teorema de Euler é o de número onze, na página 102.

> *Se* N *é um número primo com* x*, e* n *o número de partes primas com* N*, então a potência* x^n *reduzida em uma unidade sempre será divisível por* N.

O original, em Latim:

> *Si fuerit* N *ad* x *numerus primus, et* n *numerus partium ad* N *primarum, tum potestas* x^n *unitate minuta semper per numerum* N *erit divisibilis.*

A função tociente (ϕ) não é usada com seu nome, mas Euler descreve claramente o conceito, ao dizer "o número de partes primas com N" (*numerus partium ad* N *primarum*)

[7] **Teorema 7.2.** Se $\{r_1, r_2, \ldots, r_n\}$ é sistema completo (ou reduzido) de resíduos módulo m, então para qualquer k co-primo com m, o conjunto $\{kr_1, kr_2, \ldots, kr_n\}$ também é.

[8] **Teorema 6.2:** É possível somar e multiplicar as classes de equivalência: se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então

i) $a + c \equiv b + d \pmod{m}$,

ii) $ac \equiv bd \pmod{m}$.

mento, eliminando os r_i, e reescrevemos

$$a^{\phi(m)} \equiv 1 \pmod{m}. \qquad \square$$

Como $\phi(14) = 6$, o Teorema de Euler[9] garante que a sexta potência de qualquer inteiro co-primo com 14 será congruente a um módulo 14. Por exemplo,

$$9^6 = 531441 \equiv 1 \pmod{14}.$$

Teorema 7.4 (pequeno Teorema de Fermat)**.** *Se* p *é primo e* $p \nmid a$ *então*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Fermat enunciou este Teorema sem demonstração em 1640, ainda sem usar a linguagem de congruências (o que afirmou é que se p é primo e a não é divisível por p, então $a^{p-1} - 1$ é divisível por p). A demonstração foi dada por Euler em 1736; a generalização de Euler foi publicada em 1763.

O pequeno Teorema de Fermat pode ser visto como consequência direta do Teorema de Euler, já que para todo primo p, $\phi(p) = p-1$. Há outras demonstrações possíveis – pode-se usar argumentos combinatórios, por exemplo. Há também uma demonstração usando teoria de Grupos, que abordaremos mais adiante neste Capítulo.

7.2 Raízes primitivas

Considere o sistema completo de resíduos $\mathbb{Z}_{10} = \{0, 1, 2, \ldots, 9\}$. Se tomarmos o número 3, e o multiplicarmos iteradamente, vemos que

$$\begin{aligned}
3^1 &= 3 && \equiv 3 \pmod{10} \\
3^2 &= 9 && \equiv 9 \pmod{10} \\
3^3 &= 27 && \equiv 7 \pmod{10} \\
3^4 &= 81 && \equiv 1 \pmod{10} \\
3^5 &= 243 && \equiv 3 \pmod{10} \\
3^6 &= 729 && \equiv 9 \pmod{10} \\
3^7 &= 2187 && \equiv 7 \pmod{10} \\
&\vdots
\end{aligned}$$

[9] **Teorema 7.3 (de Euler):** Se $\mathrm{mdc}(a, m) = 1$ então

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Observamos que há um padrão a sequência gerada $(3, 9, 7, 1)$ se repete, e vemos que com potências de 3 conseguimos escrever $1, 3, 9, 7$ módulo 10. Mas com 3 não geramos todos os números módulo dez. Naturalmente nos perguntamos se não há algum outro que o faça.
Mais ainda, notamos que com o número 3, geramos o neutro multiplicativo, 1. Isto significa que todos os elementos no conjunto gerado, $\{1, 3, 7, 9\}$, tem inverso módulo dez! Isto acontece porque, dado 3^k neste conjunto, sempre podemos multiplicá-lo por 3^j, tal que $k + j$ sejam o expoente da próxima potência na classe de congruência do um: Temos $3^2 = 9$. Para calcular o inverso de 9, calculamos $3^9 3^x \equiv 1 \pmod{10}$. Com $x = 2$, conseguimos $3^2 3^2 = 81 \equiv 1 \pmod{10}$.
Veremos adiante que 3 é chamado de "raiz primitiva" módulo dez.
Agora, com 2 não conseguimos gerar neutro:

$$\begin{aligned}
2^1 &= 2 && \equiv 2 \pmod{10} \\
2^2 &= 4 && \equiv 4 \pmod{10} \\
2^3 &= 8 && \equiv 8 \pmod{10} \\
2^4 &= 16 && \equiv 6 \pmod{10} \\
2^5 &= 32 && \equiv 2 \pmod{10} \\
2^6 &= 64 && \equiv 4 \pmod{10} \\
&\vdots
\end{aligned}$$

Por isso, não conseguimos inversos neste conjunto.
O que observamos com as potências de 3 (mas não com as de 2) é que $3^4 \equiv 1 \pmod{10}$, e que 4 e o menor expoente inteiro positivo para o qual uma potência de 3 é congruente a 1 módulo 10. Isto nos leva à definição de ordem de um elemento em um sistema de resíduos.

Definição 7.4 (ordem de elemento em sistema de resíduos)**.** *Se h é o menor inteiro positivo tal que $a^h \equiv 1 \pmod{m}$, dizemos que a a* ***ordem***[10] *de a em m é h.* ◀

A ordem de 5 módulo 124 é, por exemplo, 3, porque $5^3 = 125$, logo $5^3 \equiv 1 \pmod{124}$.
As primeiras perguntas que fazemos são – sempre há algum elemento a tal que $a^k \equiv 1 \pmod{m}$, para algum k? E se nem sempre existe tal elemento, conseguimos determinar algum critério de existência? O Teorema 7.5 responde com exatidão estas perguntas.
)

Teorema 7.5. *Existe h tal que $a^h \equiv 1 \pmod{m}$ se e somente se $\mathrm{mdc}(a, m) = 1$.*

[10] Em terminologia mais antiga, "a pertence ao expoente h módulo m".

Demonstração. Primeiro, suponha que $\mathrm{mdc}(a, m) = 1$. Devemos ter, pelo Teorema de Euler[11], $a^{\phi(m)} \equiv 1 \pmod{m}$, portanto podemos usar $h = \phi(m)$. Agora, suponha que $a^h \equiv 1 \pmod{m}$. Como $\mathrm{mdc}(1, m) = 1$, pelo Lema 7.1[12], $\mathrm{mdc}\left(a^h, m\right) = 1$, e consequentemente $\mathrm{mdc}(a, m) = 1$. □

O final da demonstração foi feita "por extenso", mas poderia ter sido codificado em três linhas:

$$\begin{aligned} \mathrm{mdc}(1, m) &= 1 \\ \mathrm{mdc}\left(a^h, m\right) &= 1 \\ \mathrm{mdc}(a, m) &= 1 \end{aligned}$$

Damos agora nome a estas potências – o conceito de raiz primitiva é importante porque as raízes primitivas podem ser usadas para descrever completamente sistemas reduzidos de resíduos (todos os elementos no sistema são potências delas).

Definição 7.5 (raiz primitiva)**.** *Se g tem ordem $\phi(m)$ módulo m, dizemos que g é uma **raiz primitiva** módulo m.* ◀

Para $m = 14$ temos a raiz primitiva 3, porque

$$\begin{aligned} 3^1 &= 3 && \equiv 3 && \pmod{14} \\ 3^2 &= 9 && \equiv 9 && \pmod{14} \\ 3^3 &= 27 && \equiv 13 && \pmod{14} \\ 3^4 &= 81 && \equiv 11 && \pmod{14} \\ 3^5 &= 243 && \equiv 5 && \pmod{14} \\ 3^6 &= 729 && \equiv 1 && \pmod{14} \\ 3^7 &= 2187 && \equiv 3 && \pmod{14} \end{aligned}$$

O menor expoente para o qual 3^i é congruente a 1 módulo 14 é seis – que também é $\phi(14)$.

Exemplo 7.2. *Pode haver nenhuma, uma ou mais de uma raiz primitiva módulo m. Por exemplo, existe uma única raiz primitiva módulo 6, que é 5:*

$$\begin{aligned} 5^1 &\equiv 5 \pmod{6}, \\ 5^2 &\equiv 1 \pmod{6}, \end{aligned}$$

e $1, 5$ são os únicos co-primos com 6.

Mas existem oito raízes primitivas módulo 17, que são $3, 5, 6, 7, 10, 11, 12, 14$.

Exemplificamos com somente uma delas (o doze):

[11] euler

[12] **Lema 7.1:** Se $a \equiv b \pmod{m}$ e $\mathrm{mdc}(a, m) = 1$, então $\mathrm{mdc}(b, m) = 1$.

$$
\begin{aligned}
12^1 &\equiv 12 \pmod{17}, & 12^9 &\equiv 5 \pmod{17},\\
12^2 &\equiv 8 \pmod{17}, & 12^{10} &\equiv 9 \pmod{17},\\
12^3 &\equiv 11 \pmod{17}, & 12^{11} &\equiv 6 \pmod{17},\\
12^4 &\equiv 13 \pmod{17}, & 12^{12} &\equiv 4 \pmod{17},\\
12^5 &\equiv 3 \pmod{17}, & 12^{13} &\equiv 14 \pmod{17},\\
12^6 &\equiv 2 \pmod{17}, & 12^{14} &\equiv 15 \pmod{17},\\
12^7 &\equiv 7 \pmod{17}, & 12^{15} &\equiv 10 \pmod{17},\\
12^8 &\equiv 16 \pmod{17}, & 12^{16} &\equiv 1 \pmod{17}.
\end{aligned}
$$

Fica claro, portanto, que 12 *é raiz primitiva módulo* 17*. O mesmo vale para as outras raízes mencionadas (*3*,* 5*,* 6*,* 7*,* 10*,* 11 *e* 14*).* ◀

O conceito de raiz primitiva foi descrito por Gauss no Disquisitiones (no artigo 57); Gauss menciona que Euler teria inicialmente usado esse termo, e no artigo anterior (56) afirma que, além de Euler, Johann Lambert também conhecia o conceito. Mas diz também que, ao contrário de seus predecessores, ele foi o primeiro a mostrar que existem raízes primitivas para números primos[13]

Como notamos anteriormente, as classes de congruência de $3^1, 3^2, \ldots$ – e de forma geral, de $g^1, g^2, \ldots$ quando g é raiz primitiva – formam uma sequência que se repete. Temos adiante uma ilustração: na primeira linha, os g^i,

[13] No artigo 57:

> *Os números correspondentes ao expoente* $p-1$ *serão chamados de raízes primitivas, Nome dado por Euler. (...).*

O original, em Latim:

> *Numerus ad exponentem* $p-1$ *pertinentes radices primitivas cum ill. Eulero vocabimus. (...)*

No artigo 56:

> *O célebre Lambert, na dissertação já elogiada acima, menciona esta proposição, mas não aborda propriamente a necessidade de demonstração. Ninguém tentou uma demonstração, exceto o grande Euler, em comment. nov. Ac. Petrop. T. XVIII ad annum 1773, Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia p. 5 seqq vid incipimis art. 37, onde ele discorreu mais extensamente sobre a necessidade de demonstração. Mas a demonstração que o homem mais sagaz apresentou tem dois defeitos. (...)*

Em Latim:

> *Celeb. Lambert in diss. iam supra laudata acta erudit. 1769 p.127, huius propositionis mentionem facit sed demonstrationis ne necessitatem quitem attigit. Nemo vero demonstrationem tentavit praeter summum eulerum, comment. nov. Ac. Petrop. T. XVIII ad annum 1773, Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia p. 85 seqq vid imprimis art. 37 ubi de demonstrationis necessitate fusius locutus est. At demonstratio quam vir sagacissimus exhibuit duos defectus habet. (...)*

Gauss oferece duas demonstrações desse teorema no Disquisitiones, nos artigos 54 e 55.

onde g é raiz primitiva para algum módulo m; na segunda linha, $a_j < m$ representa a classe de congruencia de g^i.

$$\begin{array}{rc|cccccccccc} g^i = & & g^1 & g^2 & g^3 & \cdots & g^s & g^{s+1} & g^{s+2} & \cdots & g^{2s} & \cdots \\ \equiv & & a_1 & a_2 & a_3 & \cdots & 1 & a_1 & a_2 & \cdots & 1 & \cdots \end{array}$$

Repetimos o exemplo da raiz primitiva 3 módulo 14:

$$\begin{array}{rc|cccccccccccc} 3^i = & & 3^1 & 3^2 & 3^3 & 3^4 & 3^5 & 3^6 & 3^7 & 3^8 & 3^9 & 3^{10} & g^{11} & g^{12} & \cdots \\ \equiv & & 3 & 9 & 13 & 11 & 5 & 1 & 3 & 9 & 13 & 11 & 5 & 1 & \cdots \end{array}$$

Fica claro, então, que se $g^i \equiv 1 \pmod{m}$, então g^{ki} também será congruente a 1 módulo m. No entanto, não provamos que de fato este comportamento sempre acontece. O Teorema 7.6 trata disso, capturando portanto a característica de repetição da sequência de potências módulo m.

Teorema 7.6. *Se a ordem de a módulo m é h, e $a^k \equiv 1 \pmod{m}$, então $h \mid k$.*

Demonstração. Dividimos k por h:

$$k = qh + r, \quad 0 \leq |r| < h.$$

Agora, do enunciado temos

$$\begin{aligned} 1 &\equiv a^k && \pmod{m} \\ &\equiv a^{qh+r} && \pmod{m} \\ &\equiv (a^h)^q a^r && \pmod{m} \\ &\equiv (1)^q a^r && \pmod{m} \\ &\equiv a^r && \pmod{m} \end{aligned}$$

Mas se $a^r \equiv 1$, e $0 \leq |r| < h$, então $r = 0$, e $h \mid k$. □

A ordem de 9 módulo 14 é 3, porque

$$\begin{aligned} 9^1 = 9 &\equiv 9 && \pmod{14} \\ 9^2 = 18 &\equiv 4 && \pmod{14} \\ 9^3 = 729 &\equiv 1 && \pmod{14}. \end{aligned}$$

Mas sabemos, pelo Teorema de Euler[14], que $9^6 \equiv 1 \pmod{14}$. E como de-

[14] **Teorema 7.3 (de Euler):** Se $\mathrm{mdc}(a, m) = 1$ então

$$a^{\Phi(m)} \equiv 1 \pmod{m}.$$

termina o Teorema 7.6, $3 \mid 6$.
Uma raiz primitiva gera um conjunto de números. O próximo Teorema identifica este conjunto – é um sistema reduzido de resíduos módulo m.

Teorema 7.7. *Se g é raiz primitiva módulo m, então $g, g^2, \ldots, g^{\phi(m)}$ são um sistema reduzido de resíduos módulo m.*

Demonstração. Demonstramos que os g^i são (i) incongruentes entre si, e (ii) co-primos com m.
Começamos com a incongruência dos g^i. Suponha que existam dois elementos $g^s \equiv g^t \pmod{m}$, com $1 \leq s < t \leq \phi(m)$. Então

$$\begin{aligned} m &\mid (g^t - g^s) \\ m &\mid (g^{t-s+s} - g^s) \\ m &\mid (g^{t-s} g^s - g^s) \\ m &\mid g^s(g^{t-s} - 1). \end{aligned}$$

Mas como g é raíz primitiva módulo m, o Teorema 7.5 garante que $\operatorname{mdc}(g, m) = 1$, e $\operatorname{mdc}(g^s, m) = 1$. Concluímos que $m \nmid g^s$, e por isso

$$\begin{aligned} m &\mid (g^{t-s} - 1) \\ g^{t-s} &\equiv 1 \pmod{m} \end{aligned}$$

Então $t - s < \phi(m)$, e $g^{t-s} \equiv 1 \pmod{m}$. Mas como g é raiz primitiva, $\phi(m)$ deveria ser o menor expoente de g congruente a 1 módulo m – e chegamos a uma contradição.
Assim, todos os g^i do enunciado são incongruentes módulo m.
Passamos a outra parte da demonstração, os g^i são co-primos com m. Novamente pelo Teorema 7.5, $\operatorname{mdc}(g, m) = 1$, e evidentemente $\operatorname{mdc}\left(g^k, m\right) = 1$ também, o conjunto é um sistema reduzido de resíduos. □

Uma raiz primitiva módulo 10 é 3, porque $\phi(10) = 4$ e $3^4 \equiv 1 \pmod{10}$. Então os números 3^i, com $1 \leq i \leq 4$ são um sistema reduzido de resíduos:

$$\begin{aligned} 3^1 &\equiv 3 && \pmod{10} \\ 3^2 &\equiv 9 && \pmod{10} \\ 3^3 &\equiv 7 && \pmod{10} \\ 3^4 &\equiv 1 && \pmod{10} \end{aligned}$$

$1, 3, 7, 9$ são os quatro números menores que e co-primos com 10.
Se a tem ordem h, podemos perguntar qual é a ordem de a^k. O Teorema 7.8 e o Corolário 7.1 tratam disso, e serão úteis mais adiante para determinar a quantidade de raízes primitivas para cada m.

Teorema 7.8. *Se a ordem de* a *é* h *módulo* m*, e* $\mathrm{mdc}(j,h) = d$*, então a ordem de* a^j *módulo* m *é* h/d*.*

Cabe neste ponto um comentário, antes da demonstração. É evidente que, se a ordem de a é h módulo m, então para todo múltiplo de h (por exemplo, jh),

$$\begin{aligned} a^{jh} &\equiv (a^j)^r \\ &\equiv 1^r \\ &\equiv q \pmod{m}. \end{aligned}$$

O Teorema 7.8 aborda outros casos, onde o expoente não é múltiplo de h, e determina também a ordem de a^j: não basta que $(a^j)s \equiv 1 \pmod{m}$, queremos o *menor* s para o qual isto ocorre.

Demonstração. Se a^j tem ordem k módulo m, então

$$(a^j)^k = a^{jk} \equiv 1 \pmod{m}.$$

Pelo Teorema 7.6[15], como a ordem de a é h, então

$$h \mid kj$$

Dividimos os dois lados da relação por $\mathrm{mdc}(j,h)$:

$$\underbrace{\left(\frac{h}{\mathrm{mdc}(j,h)}\right)}_{(i)} \Big| k \underbrace{\left(\frac{j}{\mathrm{mdc}(j,h)}\right)}_{(ii)}$$

Renomeamos $d = \mathrm{mdc}(j,h)$, $H = h/d$ e $J = j/d$:

$$H \mid Jk$$

Mas como H é co-primo com J, então a relação vale se e somente se $H \mid k$:

$$H \mid k. \tag{7.1}$$

Agora,

$$\begin{aligned} a^{jH} &= a^{JHd} \\ &= a^{Jh} \\ &= (a^h)^J \\ &\equiv 1 \pmod{m} \end{aligned}$$

[15] **Teorema 7.6:** Se a ordem de a módulo m é h, e $a^k \equiv 1 \pmod{m}$, então $h \mid k$.

Mas a ordem de a^j é k, e como $(a^j)^H \equiv 1 \pmod{m}$, então

$$k \mid H. \tag{7.2}$$

Desta forma, $H \mid k$ (por 7.1) e $k \mid H$ (por 7.2), e concluimos que $k = H = h/d$. □

Por exemplo, a ordem de 5 módulo 26 é 4:

$$\begin{aligned} 5^1 &\equiv 5 && \pmod{26} \\ 5^2 &\equiv 25 && \pmod{26} \\ 5^3 &\equiv 21 && \pmod{26} \\ 5^4 &\equiv 1 && \pmod{26} \end{aligned}$$

Se perguntarmos qual deve ser a ordem de 5^6 módulo 26, usamos o Teorema 7.8 com $a = 5$, $h = 4$ e $j = 6$. Como $d = \mathrm{mdc}\,(4, 6) = 2$, a ordem de 5^6 é $h/d = 2$:

$$\begin{aligned} (5^6)^1 &\equiv 25 && \pmod{26} \\ (5^6)^2 &\equiv 1 && \pmod{26} \end{aligned}$$

Corolário 7.1. *Se g é raiz primitiva módulo m, então g^k também é raiz primitiva módulo m se e somente se $\mathrm{mdc}\,(k, \phi(m)) = 1$.*

Demonstração. A ordem de g módulo m é $\phi(m)$, por definição (g é raiz primitiva). Se $\mathrm{mdc}\,(k, \phi(m)) = 1$, então pelo Teorema 7.8, a ordem de g^k é

$$\frac{\phi(m)}{\mathrm{mdc}\,(k, \phi(m))},$$

que só pode ser igual a $\phi(m)$ se $\mathrm{mdc}\,(k, \phi(m)) = 1$. □

Como exemplo, escolhemos $m = 18$. Uma raiz primitiva módulo 18 é 5, que podemos encontrar por sucessivas tentativas (2, 3, 4 falham, e 5 gera todos os 18 elementos). Quem são as outras raízes primitivas? Certamente podem ser escritas como 5^k, porque *todo* elemento em $\mathbb{Z}_{18}$ pode. Agora, 5^k pode ser raiz primitiva módulo dezoito se e somente se k for co-primo com $\phi(18) = 6$ – ou seja, se k for 1 ou 5.

$$\begin{aligned} 5^1 &\equiv 5 && \pmod{18} \\ 5^5 &\equiv 11 && \pmod{18} \end{aligned}$$

As raízes primitivas módulo 18 são, portanto, 5 e 11.
Agora passa a ser simples contar as raízes primitivas módulo m.

Teorema 7.9. *Há exatamente zero ou $\phi(\phi(m))$ raízes primitivas modulo m.*

Demonstração. Suponha que haja raízes primitivas, e que g seja uma delas. Há $\phi(m)$ elementos no sistema reduzido de resíduos g, $g^2, \ldots, g^{\phi(m)}$. O Corolário 7.1[16] determina que g^k é raiz primitiva módulo m se e somente se k é co-primo com $\phi(m)$. Existem $\phi(\phi(m))$ elementos assim. □

Finalmente, enunciamos sem demonstração o Teorema das Raízes Primitivas, que permite determinar exatamente para quais números m existem raízes primitivas.

Teorema 7.10 (das Raízes Primitivas)**.** *Existem raízes primitivas módulo m se e somente se $m = 1$, $m = 2$, $m = 4$, $m = p^k$, ou $m = 2p^k$, onde p é primo ímpar.*

Por exemplo, 15 é produto de dois primos ímpares, e não é da forma prescrita no Teorema. Não há, portanto, raízes primitivas módulo 15.
Já $50 = (2)5^2$ é o dobro da potência de um único primo ímpar, e há $\phi(\phi(50)) = 8$ raízes primitivas módulo 50, que são $3, 13, 17, 23, 27, 37$ e 47.

7.3 Raízes primitivas com módulo primo

Apesar de não termos demonstrado o Teorema 7.10 (das raízes primitivas), podemos facilmente provar que sempre há raízes primitivas módulo p quando p é primo. De fato, já o fizemos!

Teorema 7.11. *Sempre há raízes primitivas quando o módulo é primo.*

Demonstração. Segue imediatamente do Teorema 7.5[17]. □

Também é possível tirar algumas conclusões a respeito de raízes primitivas módulo p, que serão úteis mais tarde.

Teorema 7.12. *Se g é raiz primitiva módulo $p \in \mathbb{Z}$ e p é primo, então*

$$g^{p-1} \equiv +1 \pmod{p}$$
$$g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

Demonstração. A primeira parte é o pequeno Teorema de Fermat[18].
Para a segunda parte, veja que

$$\left(g^{\frac{p-1}{2}}\right)\left(g^{\frac{p-1}{2}}\right) = g^{p-1} \equiv 1 \pmod{p}$$

[16] **Corolário 7.1:** Se g é raiz primitiva módulo m, então g^k também é raiz primitiva módulo m se e somente se $\mathrm{mdc}(k, \phi(m)) = 1$.
[17] **Teorema 7.5:** Existe h tal que $a^h \equiv 1 \pmod{m}$ se e somente se $\mathrm{mdc}(a, m) = 1$.
[18] **Teorema 7.4 (de Fermat):** Se p é primo e $p \nmid a$ então

$$a^{p-1} \equiv 1 \pmod{p}.$$

Como o número entre parênteses multiplicado por ele mesmo é congruente a um, ele deve ser congruente a $+1$ ou -1. Mas não pode ser $+1$, porque se fosse, teríamos

$$g^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

o que não pode ocorrer, porque g é raiz primitiva, e sua ordem (o *menor* expoente k tal que g^k é congruente a um) é $p-1$. Portanto, $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. □

Observe que nesta demonstração usamos o fato da equação $x^2 \equiv 1 \pmod{p}$ ter somente duas soluções módulo p ($+1$ e -1), e também o fato de haver ordem neste anel – foi crucial observar que $(p-1)/2 < (p-1)$.
Exemplificamos:

$$\begin{aligned} 2^6 = 64 \equiv 16 &\equiv -1 \pmod{13} \\ 2^{12} = 4096 &\equiv +1 \pmod{13} \end{aligned}$$

7.4 Grupos

Um grupo é uma estrutura algébrica com uma única operação[19] Os sistemas de resíduos de que tratamos são exemplos de grupos – e demonstraremos nesta seção o Teorema de Euler usando alguns fatos básicos sobre grupos.

Definição 7.6 (grupo)**.** *Um **grupo** é um conjunto onde está definida uma operação binária, que por ora denotaremos $\odot$, tal que*

(i) *$\odot$ é associativa;*

(ii) *há um neutro e no conjunto: $a \odot e = e \odot a = a$;*

(iii) *todo elemento a tem inverso $\overline{a}$, tal que $a \odot \overline{a} = e$.*

[19] A idéia de grupo foi concebida em trabalhos que investigavam solubilidade de equações, teoria de númreos e geometria. Os dois primeiros a realizar trabalhos consideráveis no desenvolvimento do conceito de grupo foram Galois[20][21] e Cauchy 1789-1857[22]. Posteriormente o conceito foi refinado por diversos outros, incluindo William Rowan Hamilton e Abel.

[22] A respeito de Galois: é muito conhecido que morreu em um duelo. Galois era muito rebelde, viveu algumas décadas após a Revolução Franecsa e envolveu-se com a política da época. O duelo não foi a primeira vez que se pôs próximo da morte. Passou por depressão, e tentou o suicídio com uma faca, mas foi desarmado por amigos. Posteriormente, iniciou um romance com uma mulher, já comprometida. O então noivo dela soube do romance, e desafiou Galois para um duelo ao nascer do sol do dia seguinte. Galois aceitou o desafio, sabendo que certamente morreria. Durante a noite, entendendo que seriam suas últimas horas, escreveu algumas cartas a amigos e passou a noite trabalhando no que hoje se conhece com a Teoria de Galois. Eram idéias que tinha já escrito e enviado a matemáticos da época (portanto é falso que ele tenha "desenvolvido completamente" toda a teoria em uma noite – mas tê-las sistematizado em poucas horas foi, ainda assim, um feito memorável). No dia seguinte, foi atingido no estômago e deixado no chão pelo adversário. O irmão de Galois chegou após o duelo, tentou socorrê-lo, mas o tempo do genial Galois já estava por se encerrar (aos vinte anos de idade).

Se a operação $\odot$ é comutativa, dizemos que o grupo é comutativo, ou "abeliano".
A quantidade de elementos em um grupo finito é chamada de ordem *do grupo.* ◀

Listamos agora alguns exemplos de grupos.

Exemplo 7.3.

- *Os inteiros, com a operação de soma: a operação é associativa; existe o neutro zero; e todo inteiro n tem inverso aditivo $-n$. O grupo é comutativo.*
- *Os reais sem o zero, com a operação de multiplicação: a operação é associativa; existe o neutro um; todo real $x \neq 0$ tem inverso multiplicativo $1/x$. O grupo é comutativo.*
- *Em um espaço vetorial, os vetores formam um grupo com a operação de soma: a operação é associativa; existe o vetor neutro zero; todo vetor v tem um inverso $-v$. Este grupo é comutativo, porque $v + w = w + v$*
- *O conjunto das matrizes com entradas reais e a mesma quantidade de linhas e colunas, usanado a operação usual de soma: a soma de matrizes é associativa, existe como neutro a matriz zero, e toda matriz A tem uma inversa aditiva $-A$. Além disso, o grupo é comutativo, porque $A + B = B + A$.*
- *O conjunto das matrizes quadradas não singulares de ordem n, com a operação de multiplicação. A multiplicação de duas matrizes não singulares resulta em outra matriz não singular*[23]*; a operação de mutiplicação de matrizes é asosciativa, $A(BC) = (AB)C$; existe o neutro multiplicativo I (a matriz identidade); e toda matriz não-singular A tem inversa A^{-1}. O grupo* não *é comutativo porque, em geral, $AB \neq BA$.*
- *Seja $(R, +, \cdot)$ um anel. Se considerarmos somente a operação de adição em R, temos um grupo (isto segue diretamente da definição de anel).*
- *Seja A um conjunto. Então o conjunto $S(A)$ de todas as bijeções $\sigma : A \to A$, de A nele mesmo (ou seja, $S(A)$ é o conjunto das permutações de A), é um grupo com a função identidade como elemento neutro; composição como operação de grupo; e função inversa como inverso de cada bijeção.*

[23] Nos outros exemplos era evidente que a operação é fechada, mas aqui faz sentido mencionar que a multiplicação não gerará uma matriz fora do conjunto que especificamos.

- *Finalmente, o conjunto unitário* $\{x\}$ *com uma operação* $x \cdot x = x$ *é um grupo. A operação é evidentemente associativa (por vacuidade); o único elemento,* x*, é o neutro, e o inverso do único elemento é ele mesmo. Além disso o grupo é, por vacuidade, comutativo.* ◀

O Teorema 7.13 nos permitirá trabalhar com expoentes da maneira usual em grupos. Sua demonstração é pedida no Exercício 183.

Teorema 7.13. *Seja* G *um grupo, onde denotamos a operação por* $\cdot$ *(da mesma forma que a multiplicação usual), e onde também denotamos por* x^a *a aplicação da operação* $a-1$ *vezes em* x*,*

$$x^a = \underbrace{x \cdot x \cdot x \cdots x}_{a-1 \text{ operações}}.$$

Em G *valem as leis usuais para expoentes:*

$$(x^a)^b = x^{ab},$$
$$x^{a+b} = x^a x^b.$$

O Teorema vale independente da comutatividade da operação, porque trata apenas de um único elemento (x).
Tanto adição como multiplicação em inteiros (e reais) são operações que podem ser usadas na definição de um grupo, e em diferentes situações pode-se usar uma ou outra notação. Nesta situação, as leis de cancelamento são

$$(a(b(x)) = (ab)x,$$
$$(a+b)x = ax + bx.$$

No exemplo a seguir é possível não apenas perceber que as leis de expoentes valem, mas também observar o funcionamento da estrutura de grupo.

Exemplo 7.4. *Seja* $(G, \odot)$ *um grupo, com*

$$G = \{e, a, b, c\}$$

e $\odot$ *dada pela tabela a seguir.*

$\odot$	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

Verificamos que $c^5 = c^2 \odot c^3$*. No desenvolvimento, os trechos sublinhados*

correspondem àqueles onde a operaçõa será aplicada.

$$\begin{aligned} c^5 &= \underline{c \odot c} \odot c \odot c \odot c \\ &= \underline{a \odot c} \odot c \odot c \\ &= \underline{d \odot c} \odot c \\ &= \underline{b \odot c} \\ &= e. \end{aligned}$$

Da mesma forma,

$$\begin{aligned} c^2 &= \underline{c \odot c} \\ &= a, \\ c^3 &= \underline{c \odot c} \odot c \\ &= \underline{a \odot c} \\ &= d, \end{aligned}$$

portanto $c^2 \odot c^3 = a \odot d = e$.
Observamos também que o grupo é comutativo, porque a tabela é simétrica.
◀

Teorema 7.14. *Todo sistema reduzido de resíduos módulo* n *é um grupo comutativo com a operação de multiplicação módulo* n*, com neutro igual a um. A ordem do grupo é* $\phi(n)$.

Demonstração. Se a, b pertencem a um sistema reduzido de resíduos módulo m, então $\mathrm{mdc}(a, m) = \mathrm{mdc}(b, m) = 1$. Isto significa que $\mathrm{mdc}(ab, m)$ também é um, e ab tem representante de sua classe de congruência no sistema. Assim, a operação é fechada no conjunto.
A multiplicação é associativa; existe o elemento neutro 1, ou algum $x \equiv 1 \pmod{m}$ no sistema; falta somente verificar que todo elemento tem inverso. O inverso de um elemento a é $\overline{a}$, tal que $a\overline{a} \equiv 1 \pmod{m}$. Esta equação tem solução se e somente se $\mathrm{mdc}(a, m) = 1$ – o que é verdadeiro. □

O Teorema 7.6[24] pode ser visto como caso particular do Teorema 7.15, para grupos.

Teorema 7.15. *Seja* x *um elemento de ordem* n *em um grupo, e suponha que* $x^k = 1$*, com* k *inteiro positivo. Então* $n \mid k$.

Demonstração. Expresse a divisão de k por n como $k = nq + r$, com q, r

[24] **Teorema 7.6:** Se a ordem de a módulo m é h, e $a^k \equiv 1 \pmod{m}$, então $h \mid k$.

inteiros positivos e $0 \leq r < n$. Então

$$\begin{aligned} 1 &= x^k \\ &= x^{nq+r} \\ &= (x^n)^q x^r \\ &= x^r, \end{aligned}$$

então $r = 0$ e $n \mid k$. □

Em nossa discussão sobre raízes primitivas verificamos que as potências $g^1, g^2, \ldots$ formam um padrão que se repete ciclicamente. Isto acontece porque para algum n, $g^n = g$. Dizemos que grupos como este são *cíclicos*.

Definição 7.7 (grupo cíclico)**.** *Um grupo é **cíclico** se todos seus elementos podem ser esritos como potência de algum elemento:* $x = ggg\ldots g = g^n$*, para algum* n*. Um elemento* g *usado desta forma para descrever todos os outros é um gerador do grupo.* ◀

Evidentemente as raízes primitivas em sistemas reduzidos de resíduos são geradores, o que significa que estes sistemas são grupos cíclicos.

Teorema 7.16. *Um sistema reduzido de resíduos é um grupo cíclico.*

Demonstração. Uma raiz primitiva módulo m gera o sistema reduzido de resíduos. □

Com os conceitos apresentados até aqui já é possível enunciar o Teorema 7.17 (objeto do Exercício 188).

Teorema 7.17. *Se* p *é primo,* p *não divide nenhuma potência de* b*, e a expansão de* $1/p$ *na base* b *tem período* k*, então* k *é a ordem de* b *módulo* p*.*

Exemplo 7.5. *Neste exemplo a parte periódica da expansão em dígitos é mostrada com barra superior:* $0.3480808080\ldots = 0.34\overline{80}$*.*
Na base dez,

$$\begin{aligned} 1/3 &= 0.\overline{3} && \text{per} = 1 \\ 1/7 &= 0.\overline{142857} && \text{per} = 6 \\ 1/11 &= 0.\overline{09} && \text{per} = 2 \\ 1/13 &= 0.\overline{076923} && \text{per} = 6 \\ 1/17 &= 0.\overline{0588235294117647} && \text{per} = 16 \end{aligned}$$

Para cada período k*, a ordem de* 10^k *módulo* p *é* k*:*

$$\begin{aligned}
10^1 &= 10 && \equiv 1 \pmod{3}\\
10^6 &= 1000000 && \equiv 1 \pmod{7}\\
10^2 &= 100 && \equiv 1 \pmod{11}\\
10^6 &= 1000000 && \equiv 1 \pmod{13}\\
10^{16} &= 10000000000000000 && \equiv 1 \pmod{17}
\end{aligned}$$

Não há potências de 10 *menores que resultem em um módulo esses primos (ou seja, de fato esta é a ordem de* $10^k \pmod p$*).*
Da mesma forma, na base 3*,*

$$\begin{aligned}
1/5 &= 0.\overline{0121} && \text{per} = 4\\
1/7 &= 0.\overline{010212} && \text{per} = 6\\
1/11 &= 0.\overline{00211} && \text{per} = 5\\
1/13 &= 0.\overline{002} && \text{per} = 3\\
1/17 &= 0.\overline{0000112021221102 01} && \text{per} = 16
\end{aligned}$$

Para cada período k*, a ordem de* 3^k *módulo* p *é* k*:*

$$\begin{aligned}
3^4 &= 81 && \equiv 1 \pmod{5}\\
3^6 &= 729 && \equiv 1 \pmod{7}\\
3^5 &= 243 && \equiv 1 \pmod{11}\\
3^3 &= 27 && \equiv 1 \pmod{13}\\
3^{16} &= 43046721 && \equiv 1 \pmod{17}
\end{aligned}$$

Também não há potências de 3 *menores que estas, resultando em* 1 *módulo estes primos.* ◀

É natural a definição de subgrupo – um grupo dentro de outro grupo.

Definição 7.8 (subgrupo)**.** *Seja* G *um grupo. Um subconjunto* H *de* G *é* ***subgrupo*** *de* G *se também ele é grupo, com a mesma operação.* ◀

As matrizes triangulares inferiores formam um grupo com a operação de adição, portanto são um subgrupo do grupo de todas as matrizes.
Os inteiros pares com a operação de soma formam um subgrupo de $\mathbb{N}$.
As matrizes quadradas (com ordem n fixa) com determinante ± 1 formam

um grupo com a operação de multiplicação – um subgrupo do grupo das matrizes não singulares.

Teorema 7.18 (de Lagrange)**.** *A ordem de um subgrupo divide a ordem do grupo.*

O Teorema de Lagrange é um dos resultados mais elementares em Teoria de Grupos – mas com ele já podemos elaborar uma demonstração mais interessante do Teorema de Euler.

Demonstração do Teorema de Euler. Seja $a < n$, co-primo com n. Então as potências de a módulo n – $a, a^2, \ldots, a^t \pmod n$ – formam um subgrupo, onde $a^t \equiv a^0 \equiv 1 \pmod n$. De acordo com o Teorema de Lagrange, $t \mid \phi(n)$ (ou seja, $kt = \phi(n)$). Então

$$\begin{aligned} a^{\phi(n)} &\equiv a^{kt} \\ &\equiv (a^t)^k \\ &\equiv 1^k \\ &\equiv 1 \pmod n. \end{aligned}$$ □

É também interessante comparar o Teorema de Lagrange com o Teorema 7.6[25].

7.4.1 O grupo de unidades

Se n não é primo, nem todo elemento em $\mathbb{Z}_n$ tem inverso (ou seja, nem todos são unidades). Quando escolhemos apenas as unidades em $\mathbb{Z}_n$, obtemos um sistema reduzido de resíduos onde todos os elementos tem inverso – este é o *grupo de unidades módulo* n.

Definição 7.9 (grupo de unidades módulo n)**.** *Para todo inteiro positivo n, definimos o* ***grupo de unidades módulo*** n *como o subconjunto de $\mathbb{Z}_n$ onde todos os elementos são unidades módulo n; a operação de grupo é a multiplicação módulo n. Denotamos este grupo por U_n.* ◀

Exemplo 7.6. *As unidades módulo 10 são $1, 3, 7, 9$, portanto estes são os elementos do grupo U_{10}, onde a operação de grupo é a multiplicação módulo 10.* ◀

Teorema 7.19. *O grupo U_n é cíclico.*

A demonstração do Teorema 7.20 é pedida no Exercício 199.

Teorema 7.20. *Seja n um inteiro positivo. Então $\mathbb{Z}_{\phi n}$ é grupo com a operação de multiplicação; além disso, U_n é isomorfo a $\mathbb{Z}_{\phi n}$.*

[25] **Teorema 7.6:** Se a ordem de a módulo m é h, e $a^k \equiv 1 \pmod m$, então $h \mid k$.

7.5 Raízes da Unidade

Uma *raiz da unidade* (ocasionalmente chamadas também de *número de de Moivre*[26]) é uma solução para a equação $x^n - 1 = 0$. Em $\mathbb{R}$ há somente as soluções $+1, -1$ quando n é par, ou somente $+1$ quando n é ímpar. Em outras estruturas há mais raízes. Por exemplo, em $\mathbb{C}$, com $n = 5$, temos as cinco raízes distintas

$$1, e^{\pm\frac{2i\pi}{5}}, e^{\pm\frac{4i\pi}{5}}.$$

Neste texto, trabalharemos em $\mathbb{C}$.

Definição 7.10 (raiz da unidade)**.** *Uma **raiz da unidade** (ou ainda, n-**ésima raiz da unidade**) é um número $z \in \mathbb{C}$ tal que $z^n = 1$.* ◀

Exemplo 7.7. *As raízes terceiras da unidade são as raízes da equação $x^3 - 1 = 0$, ou seja,*

$$1, \frac{-1 - i\sqrt{3}}{2}, \frac{-1 + i\sqrt{3}}{2}.$$ ◀

Evidentemente, se $x^2 = 1$, a norma de x é 1. Isso significa que, no plano complexo, x é representado por um ponto na circunferencia de raio um centrada na origem. As figuras a seguir ilustram, no plano complexo, raízes da unidade para $n = 3$, $n = 4$ e $n = 5$ (para preservar a clareza da figura, os valores para $n = 5$ não são incluídos).

[26] Abraham de Moivre (1667-1754, francês), mudou-se para a Inglaterra ainda jovem devido a perseguição religiosa – a prática do protestantismo cristão foi declarada ilegal pelo impoerador Luís XIV) publicou, por volta de 1730, um artigo onde constrói a fórmula[27] que hoje tem seu nome,

$$(\cos\theta + i\,\mathrm{sen}\,\theta)^n = \cos(n\theta) + i\,\mathrm{sen}(n\theta),$$

que permitiu a obtenção das raízes n-ésimas de 1, com $\theta = 2k\pi/n$. A publicação se chamava Miscellanea Analytica.

De Moivre, Abraham. **Miscellanea Analytica de Seriebus et Quadraturis**. Londres: J. Tonson & J. Watts, 1730.

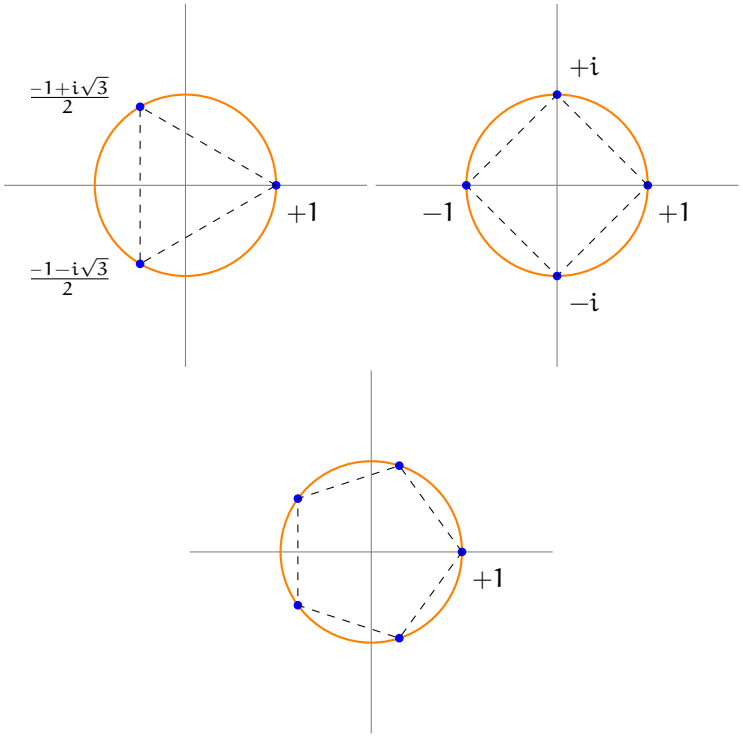
De Moivre não incluiu a fórmula como a conhecemos no texto; ela pode ser derivada do primeiro lema do livro (na página um), que usava idéias de seu amigo pessoal, Isaac Newton. Posteriormente, Euler (1707-1783) apresentou a conhecida fórmula exponencial,

$$e^{i\theta} = \cos\theta + i\,\mathrm{sen}\,\theta,$$

consolidando a ponte entre trigonometria e teoria dos números.
O uso das raízes da unidade no contexto de Teoria dos Números e polinômios só aconteceu no Século XIX com Gauss.

[27] Mais tarde, a função cis foi definida como

$$\mathrm{cis}(\theta) = \cos(\theta) + i\,\mathrm{sen}(\theta).$$



As raízes da unidade são equidistantes e definem, portanto, polígonos regulares[28]. De fato, a multiplicação de um número complexo por uma n-ésima raiz da unidade é equivalente a rotação, no plano complexo, por um ângulo de $2\pi/n$.

Teorema 7.21. *As n-ésimas raízes da unidade são*

$$e^{\frac{2ki\pi}{n}}, \qquad k = 1, 2, \ldots, n.$$

Demonstração. A fórmula de Euler nos garante que

$$e^{2i\pi} = \cos(2\pi) + i\,\mathrm{sen}(2\pi) = 1.$$

[28] Gauss estudou as raízes da unidade e sua relação com a construção de polígonos regulares, apontando várias consequencias, inclusive uma investigação a respeito da construtibilidade de polígonos regulares com régua e compasso, e uma demonstração do Lei da Reciprocidade Quadrática (exposta no Capítulo 9).

Gauss, Johann Carl Friedrich. **Disquisitiones Arithmeticae**. [*S. l.*], 1801. Seção VII, "Equações definindo seções de um círculo".

Agora, 1 elevado a qualquer potência permanece 1, logo

$$\left(e^{2i\pi}\right)^r = \left(e^{2i\pi}\right)^r = 1^r = 1.$$

Para valores de $k \in \mathbb{N}$, portanto, o valor permanece 1:

$$\begin{aligned}
\left(e^{2i\pi}\right)^1 &= e^{2i\pi} = 1^1 = 1 \\
\left(e^{2i\pi}\right)^2 &= e^{4i\pi} = 1^2 = 1 \\
\left(e^{2i\pi}\right)^3 &= e^{6i\pi} = 1^3 = 1 \\
\left(e^{2i\pi}\right)^4 &= e^{8i\pi} = 1^4 = 1 \\
&\vdots
\end{aligned}$$

Mas se extraírmos a n-ésima raiz. teremos uma unidade (*não* necessariamente $+1$):

$$(z^n)^{\frac{1}{n}} = z = e^{\frac{2ki\pi}{n}}$$

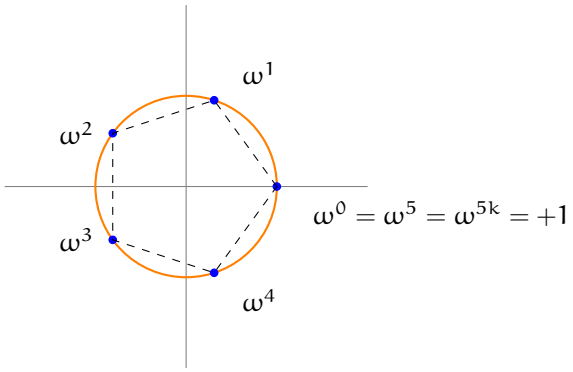
Tendo fixado n, podemos variar k, e haverá n possibilidades distintas para raízes da unidade, porque $n/n = 1$, e portanto

$$e^{\frac{2ni\pi}{n}} = e^{2i\pi} = 1 = e^{\frac{2(1)ni\pi}{1}}. \qquad \square$$

O Teorema 7.21 nos permite simplificar a notação: fixado n, definimos

$$\omega = e^{\frac{2i\pi}{n}}$$

e usaremos a notação ω^i, $i = 0, \ldots, n-1$ para as raízes n-ésimas da unidade.



Para todo $k \in \mathbb{Z}$:

$$\begin{aligned}
\omega^0 &= \omega^{5k} \\
\omega^1 &= \omega^{5k+1} \\
\omega^2 &= \omega^{5k+2} \\
\omega^3 &= \omega^{5k+3} \\
\omega^4 &= \omega^{5k+4}
\end{aligned}$$

Fica bastante claro a partir da figura que as raízes da unidade formam um grupo cíclico onde o gerador é ω. A operação de grupo é a mutiplicação por ω, ou ainda, uma rotação[29] por $2\pi/n$. O Teorema 7.22 explicita isso (a demonstração é pedida no Exercício 204).

Teorema 7.22. *Fixado n, as raízes da unidade formam um grupo.*

Fica claro agora o motivo das raízes da unidade estarem equidistantes no círculo unitário: cada uma representa uma rotação por $2\pi/n$.
O Teorema 7.23 esclarece a relação entre raízes de unidades e sistemas completos de resíduos (que já foi apontada quando afirmamos, no Teorema 7.22, que elas formam um grupo).

Teorema 7.23. *Fixado n, então $\{\omega^{t_0}, \omega^{t_1} \ldots, \omega^{t_{n-1}}\}$ é o conjunto de n-ésimas raízes da unidade se e somente se $\{t_0, t_1, \ldots, t_{n-1}\}$ é um sistema completo de resíduos módulo n.*

Demonstração. Inicialmente mostramos que se os t_i formam um sistema completo de resíduos, os ω^{t_i} são todas as n-ésimas raízes da unidade.
Usamos a definição de sistema completo de resíduos. Se $\{t_0, t_1, \ldots, t_{n-1}\}$ é um sistema completo de resíduos módulo n, então o conjunto $\{t_0, t_1, \ldots, t_{n-1}\}$ tem elementos congruentes a $\{0, 1, \ldots, n\}$. Isso significa que para cada $s_j \in \{0, 1, \ldots, n-1\}$ existe exatamente um t_j congruente a s_j módulo n. Isso é o mesmo que dizer que, para todo j existe um inteiro l_j tal que

$$\omega^{t_j} = \omega^{nl_j+s_j} = \left(e^{\frac{2i\pi}{n}}\right)^{nl_j+s_j} = e^{2i\pi l_j + \frac{2i\pi s|j}{n}} = e^{2i\pi l_j} e^{\frac{2i\pi s|j}{n}} = \left(e^{\frac{2i\pi}{n}}\right)^{s_j} = \omega^{s_j}.$$

Ou seja, para todo inteiro $s_j \in \{0, 1, \ldots, n-1\}$ temos que ω^{t_j} será igual a um ω^{s_j} diferente. Como são exatamente n as n-ésimas raízes da unidade, então o conjunto de expoentes $\{t_0, \ldots, t_{n-1}\}$ gera todas elas.
Falta mostrarmos que se os ω^{t_i} são exatamente as n raízes n-ésimas da unidade, então os t_i formam um sistema completo de resíduos.
Suponha que $\{t_0, \ldots, t_{n-1}\}$ não é sistema completo de resíduos módulo n. Como há n elementos, isso significa que deve haver dois elementos no con-

[29] Uma rotação por θ radianos é obtida ao multiplicar um núero complexo por $e^{i\theta}$; assim, a multiplicação por $\omega = e^{(i2\pi)/n}$ é uma rotação por $2\pi/n$.

junto que são congruentes módulo n: $t_u \equiv t_v \pmod{n}$, ou seja, para algum k,

$$t_u = nk + t_v.$$

Assim teremos

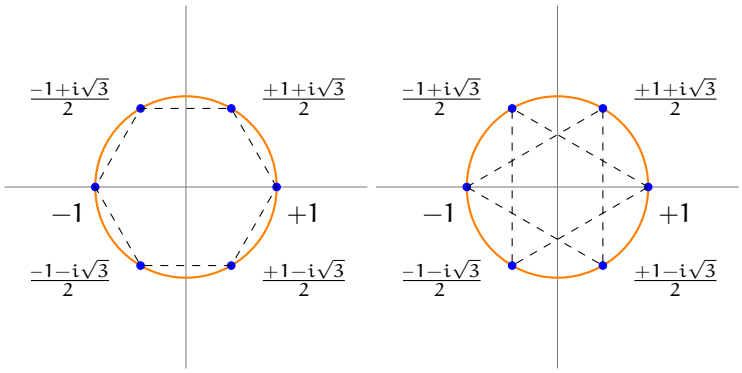
$$\omega^{t_u} = \omega^{nk+t_v} = \omega^{t_v},$$

e não teremos todos os n distintos ω^{t_i}. □

Definição 7.11 (ordem de raiz da unidade)**.** *Se ω é raíz n-ésima da unidade, mas não é raiz da k-ésima da unidade para nenhum $k < n$, então n é a* ***ordem*** *de ω enquanto raiz da unidade.* ◀

Definição 7.12 (raiz primitiva da unidade)**.** *Uma* ***n-ésima raiz primitiva da unidade*** *é uma n-ésima raiz da unidade que não é k-ésima raiz da unidade para nanhum $k < n$. Ou ainda, uma raiz n-ésima da unidade é primitiva se sua ordem é n. Denotamos raízes primitivas por ζ.* ◀

A representação geométrica das raízes da unidade no plano complexo é bastante útil neste momento. A figura a seguir ilustra as raízes sextas da unidade. Não usamos a notação ω^i aqui para que seja fácil observar o que ocorre com as partes real a imaginária dos pontos.



A figura da direita mostra que, geometricamente, as raízes sextas são as mesmas que as terceiras, mas incluindo as reflexões pelo eixo das ordenadas (o que significa que adicionamos os mesmos números, mas trocando o sinal da parte real).

É interessante que observamos que as raízes da unidade, quando representadas no plano complexo, são equidistantes. Isso significa que, se n é ímpar, sabendo que $+1$ sempre é raiz da unidade, as raízes n-ésimas formarão um polígono regular posicionado de maneira assimétrica em relação ao eixo das ordenadas (o que pode ser facilmente visto nos casos $n = 3$ e $n = 5$, já ilustrados). E as raízes $2n$-ésimas incluirão as raízes n-ésimas com os sinais da parte real trocados (geometricamente fazendo uma reflexão no eixo das

ordenadas, como observamos), definindo assim um polígono simétrico nos dois eixos.

Dentre as raízes sextas da unidade há duas que são primitivas,

$$\frac{+1 \pm i\sqrt{3}}{2},$$

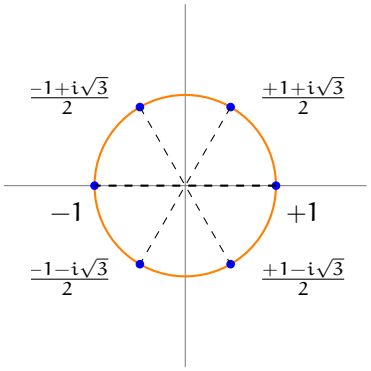
e as outras são também raízes n-ésimas para $n < 6$:

$$+1 \qquad n = 1 \tag{7.3}$$

$$-1 \qquad n = 2 \tag{7.4}$$

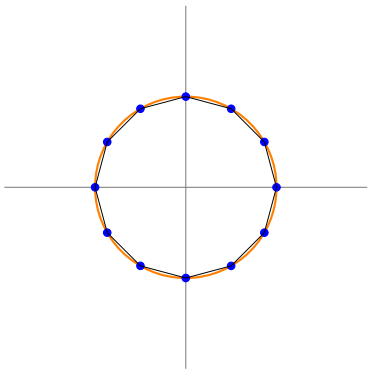
$$\frac{-1 \pm i\sqrt{3}}{2} \qquad n = 3 \tag{7.5}$$

Ainda construindo a intuição, observamos que as raízes sextas são $6 = 3 \cdot 2$ – duas vezes as raízes terceiras (refletidas). Mas podemos olhar de outra forma: são **tres** vezes as raízes quadradas, rotacionadas por $2\pi/n$:

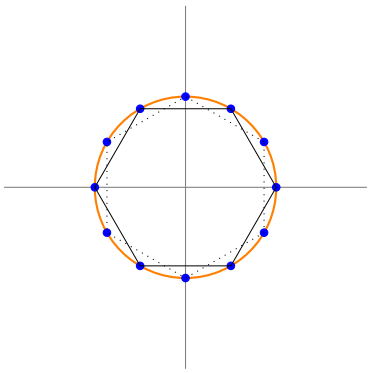


Estamos olhando para os divisores de seis! E, assim como 2 divide todo número par, todo conjunto de raízes primitivas da unidade pode ser descrito como $n/2$ vezes o par $(-1, 1)$, rotacionado $n/2$ vezes por um ângulo de $2\pi/n$ (é interessante rever a figura para $n = 4$, e imaginar a de $n = 10$). Se n tiver mais fatores, poderemos rotacionar as raízes de ordem anterior para obter as raízes n-ésimas.

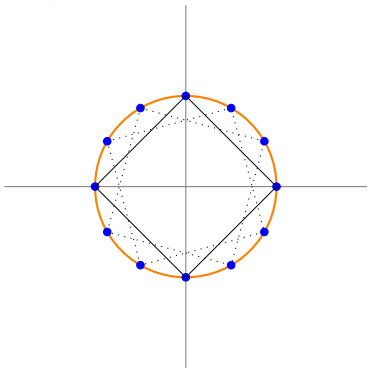
A próxima figura ilustra este fato para os divisores de 12. O caso 1×12 é simplesmente o dodecágono instrito; o caso 1×12 é o conjunto de raízes da unidade, isolados – porque a raiz 1-ésima de um é somente $+1$, e o que se faz é rotacionar o complexo $1 + 0i$ doze vezes.



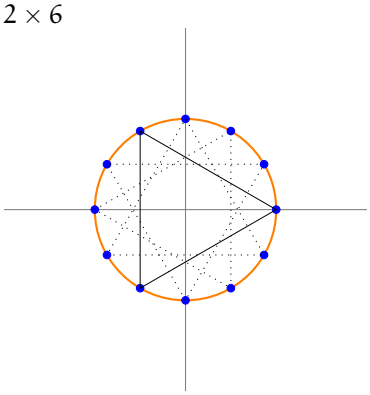
1×12



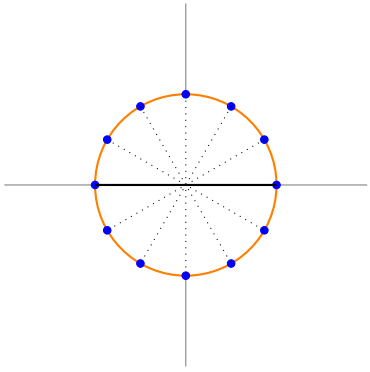
2×6



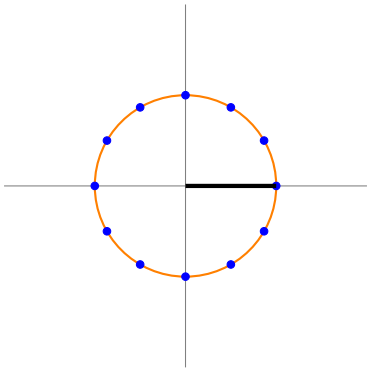
3×4



4×3



6×2



12×1

Uma raiz da unidade é primitiva, portanto, se participa da fatoração de n, mas não das raízes de ordem anterior a n. Isso já nos motiva a enunciar o próximo Teorema.

Teorema 7.24. *As n-ésimas raízes primitivas da unidade são*

$$e^{\frac{2ki\pi}{n}}, \qquad k = 1, 2, \ldots, n, \quad \text{mdc}\,(k, n) = 1.$$

A quantidade de n-ésimas raízes primitivas da unidade é, portanto, $\phi(n)$. A intuição nos indica que um análogo do Teorema 7.23[30] deve valer para sistemas reduzidos de resíduos, e portanto enunciamos o Teorema 7.25 (demonstração pedida no Exercício 206). As mudanças realizadas a partir do enuncaiado do Teorema 7.23 estão sublinhadas.

Teorema 7.25. *Fixado n, então $\{\zeta^{t_0}, \zeta^{t_1}, \ldots, \zeta^{t_k}\}$, onde $k = \phi(n) - 1$, é o conjunto de n-ésimas raízes primitivas da unidade se e somente se $\{t_0, t_1, \ldots, t_k\}$ é um sistema reduzido de resíduos módulo n.*

Exercícios

Ex. 173 — Prove que em uma lista de $k+1$ números $a_1, a_2, \ldots, a_{k+1}$ há pelo menos dois números, a_i e a_j, tais que $(a_i - a_j) \mid k$.

Ex. 174 — Encontre todas as raízes primitivas módulo 5, 7, 9, e 11.

Ex. 175 — Mostre um sistema completo de resíduos módulo 13 contendo somente inteiros ímpares.

Ex. 176 — Suponha que $a^{n-1} \equiv 1 \pmod{n}$ mas que, para todo d divisor próprio de $n-1$, $a^d \not\equiv 1 \pmod{n}$. Prove que n é primo.

Ex. 177 — Prove que se $\{a_1, a_2, \ldots, a_k\}$ é um sistema reduzido de resíduos módulo p, então $\{\overline{a_1}, \overline{a_2}, \ldots, \overline{a_k}\}$, onde $\overline{a_i}$ é o inverso de a_i módulo p, também é.

Ex. 178 — Seja $\{a_1, a_2, \ldots, a_k\}$ um sistema reduzido de resíduos módulo m (e portanto $k = \phi(m)$). Prove que $\{a_1^r, a_2^r, \ldots, a_k^r\}$ também é sistema reduzido de resíduos se e somente se $\mathrm{mdc}\,(r, \phi(m))$.

Ex. 179 — Seja p primo. Prove que 1 e $p-1$ são os únicos números no conjunto $\{0, 1, \ldots, p-1\}$ cujos quadrados são congruentes a um módulo p.

Ex. 180 — Sejam a, b raízes primitivas módulo p, um primo ímpar. Prove que ab não pode ser raiz primitiva módulo p.

Ex. 181 — Prove que se p é um primo ímpar e a tem ordem $2k$ módulo p, então $a^k \equiv -1 \pmod{p}$.

Ex. 182 — Prove que o conjunto dos inteiros módulo m, para todo $m \geq 0$, é um grupo comutativo com a operação de soma módulo m.

Ex. 183 — Demonstre o Teorema 7.13.

[30] Teorema 7.23: Fixado n, então $\{\omega^{t_0}, \omega^{t_1} \ldots, \omega^{t_{n-1}}\}$ é o conjunto de n-ésimas raízes da unidade se e somente se $\{t_0, t_1, \ldots, t_{n-1}\}$ é um sistema completo de resíduos módulo n.

Ex. 184 — O conjunto $G = \{a, b, c, d, e\}$, com a operação a seguir é um grupo? Se for, é comutativo?

$\odot$	e	a	b	c	d
e	e	a	b	c	d
a	a	e	c	d	b
b	b	d	e	a	c
c	c	b	d	e	a
d	d	c	a	b	e

Ex. 185 — Seja $m > 2$. Os números $1^2, 2^2, 3^2, \ldots, m^2$ formam um sistema completo de resíduos módulo m?

Ex. 186 — Seja p um primo ímpar, e sejam $\{s_1, s_2, \ldots, s_{p-1}\}$ e $\{t_1, t_2, \ldots, t_{p-1}\}$ dois sistemas completos de resíduos módulo p. Prove que $\{s_1t_1, s_2t_2, \ldots, s_kt_k\}$ não pode ser sistema completo de resíduos módulo p.

Ex. 187 — Se p é um primo ímpar e g é raiz primitiva módulo p^k, quando g também seria raiz primitiva módulo $2p^k$?

Ex. 188 — Prove o Teorema 7.17.

Ex. 189 — (Olimpíada Matemática de São Petersburgo) Prove que $m \mid \phi(a^m - 1)$ para todos os inteiros a e m.

Ex. 190 — Seja $n \in \mathbb{Z}$ tal que $3 \nmid n$ ou tal que $9 \mid n$. Prove que $n^7 \equiv n \pmod{63}$.

Ex. 191 — Sejam a, b co-primos. Prove que $\{0, a, 2a, 3a, \ldots, (b-a)a\}$ é um sistema completo de resíduos módulo b.

Ex. 192 — Mostre que se $a_1, a_2, \ldots, a_k$ é um sistema reduzido de resíduos módulo m, onde $m > 2$, então $\sum_i a_i \equiv 0 \pmod{m}$.

Ex. 193 — Prove que para todo inteiro positivo n maior que um, $n \mid \phi(2^n - 1)$.

Ex. 194 — Seja p primo e $\{a_1, a_2, \ldots, a_k\}$ um sistema completo de resíduos módulo p. Prove que para todo inteiro n existe r tal que

$$n = \sum_{i=0}^{r} x_i p^i \pmod{p^{r+1}},$$

onde x_i é algum dos a_i.

Ex. 195 — Suponha que $p > 3$ seja primo. Prove que o produto das raízes primitivas entre 1 e $p-1$ módulo p é congruente a 1 módulo p.

Ex. 196 — Prove que se $\mathrm{mdc}(a, b) = 1$ e a ordem de a módulo b é ts, então a ordem de b^s em a é t.

Ex. 197 — Dois grupos $(G, \odot)$ e $(H, \boxdot)$ são isomorfos se existe uma bijeção entre eles que preserva estrutura – ou seja, se existe $f : G \to H$ bijetora tal que $\forall a, b \in G$, $f(a \odot b) = f(a) \boxdot f(b)$.

(a) Prove que os grupos aditivos definidos por dois sistemas completos de resíduos com o mesmo módulo são isomorfos, e que por isso podemos tratá-los como se fossem um só: "*o* sistema completo de resíduos módulo m".

(b) Faça o mesmo com grupos multiplicativos definidos por sistemas reduzidos de resíduos.

Ex. 198 — Suponha que g seja raiz primitiva módulo p^k. Prove que g também é raiz primitiva módulo p.

Ex. 199 — Demonstre o Teorema 7.20.

Ex. 200 — Prove que em qualquer grupo, todo elemento tem um único inverso.

Ex. 201 — Seja $C \subset \mathbb{R}^2$ o conjunto de pontos da circunferência unitária,

$$C = \{(x, y) \mid x^2 + y^2 = 1\}.$$

Este conjunto pode ser um grupo, onde

- $e = (1, 0)$ é o elemento neutro;
- o inverso de cada ponto (x, y) é $\overline{(x, y)} = (x, -y)$.

a) Determine uma operação de grupo.

b) Verifique que o mesmo vale se trocarmos $\mathbb{R}$ por qualquer corpo.

Ex. 202 — (Apostol) Seja S um sistema reduzido de resíduos módulo m. Seja $d \in \mathbb{N}$, tal que $d > 0$ e $d \mid m$. Prove que:

i) S é a união de $\phi(m)/\phi(d)$ conjuntos distintos, cada um sendo um sistema reduzido de resíduos módulo d;

ii) S é a união de $\phi(d)$ conjuntos distintos, cada um tendo tamanho $\phi(m)/\phi(d)$ números congruentes uns aos outros módulo d.

Ex. 203 — Prove que a soma das n-ésimas raízes da unidade (não somente as primitivas) é zero.

Ex. 204 — Demonstre o Teorema 7.22.

Ex. 205 — Prove que se p é primo e existe uma n-ésima raiz *primitiva* da unidade em $\mathbb{Z}_p$, então $n \mid (p-1)$.

Ex. 206 — Demonstre o Teorema 7.25.

Capítulo 8

Funções Aritméticas

Propriedades importantes dos números inteiros podem ser estudadas através de funções, que tem domínio igual aos inteiros positivos. Este é o fundamento da *Teoria Analítica de Números*, onde métodos de Análise são usados na obtenção de resultados.

A Teoria Analítica de Números inicia com os trabalhos de Euler[1] sobre a série $1 + 1/2^s + 1/3^s + \cdots$ (a função que posteriormente ficou conhecida como "zeta de Riemann")[2] e sua expressão como produto[3], pela primeira vez mostrando uma conexão entre números primos e um produto infinito. No Século

[1] Leonard Euler (1707-1783), Suíço.

[2] A função zeta (ζ) de Riemman é

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

onde $s \in \mathbb{C}$, e $\mathrm{Re}(s) > 1$.

[3] O artigo é:

Euler, Leonhard. Variae observationes circa series infinitas. **Commentarii academiae scientiarum Petropolitanae**, v. 9, p. 160–188, 1744.

O Teorema 8 tem o enunciado

> *A expressão formada pela sequência de númreos primos*
>
> $$\frac{2^n \cdot 3^n \cdot 5^n \cdot 7^n \cdot 11^n \cdots}{(2^n - 1) \cdot (3^n - 1) \cdot (5^n - 1) \cdot (7^n - 1) \cdot (11^n - 1) \cdots}$$
>
> *tem o mesmo valor que a soma da série*
>
> $$1 + \frac{1}{2^n} + \frac{1}{3^n} + \frac{1}{4^n} + \frac{1}{5^n} + \frac{1}{6^n} + \frac{1}{7^n} + \cdots$$

O original:

> *Si ex ferie numerorum primorum fequens formetur expreſſio*
>
> $$\frac{2^n \cdot 3^n \cdot 5^n \cdot 7^n \cdot 11^n \cdot \mathrm{etc.}}{(2^n - 1) \cdot (3^n - 1) \cdot (5^n - 1) \cdot (7^n - 1) \cdot (11^n - 1) \cdot \mathrm{etc.}}$$

IX, Dirichlet[4] introduziu outros conceitos (caracteres e L-funções), usando métodos analíticos para provar que há infinitos primos da forma $ak + b$, para a, b co-primos[5]. Em 1859, Bernhard Riemann[6] publicou um artigo[7] estudando as propriedades da função anteriormente abordada por Euler, dando-lhe o nome de zeta (ζ), transformando um problema aritmético clássico (a contagem de primos menores do que um dado inteiro) em um problema de Análise, e estabelecendo definitivamente a área conhecida como "Teoria Analítica de Números".

Definição 8.1 (função aritmética)**.** *Uma* ***função aritmética*** *é uma função que tem os inteiros positivos como domínio, e complexos como contradomínio.* ◀

Não usaremos funções aritméticas com contradomínio complexo neste texto – será suficiente restringir a atenção a funções com contradomínio real.

Exemplo 8.1. *Funções simples tendo inteiros positivos como domínio, como* $f(n) = 2n$ *são funções aritméticas. Também a função que dá o* n*-ésimo dígito de* π *é função aritmética. Da mesma forma,*

$$f(n) = \begin{cases} +1 & \textit{se o } n\textit{-ésimo dígito de } \pi \textit{ é par} \\ -1 & \textit{se o } n\textit{-ésimo dígito de } \pi \textit{ é ímpar} \end{cases}$$

é função aritmética. ◀

Definição 8.2 (delta de Kronecker)**.** *Uma função aritmética fundamental é a função* δ*, que é a função característica do conjunto* $\{1\}$*, também conhecida como "*δ *de Kronecker":*

$$\delta(n) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{em outros casos} \end{cases}$$ ◀

erit eius valor arqualis fummae huius feriei

$$1 + \frac{1}{2^n} + \frac{1}{3^n} + \frac{1}{4^n} + \frac{1}{5^n} + \frac{1}{6^n} + \frac{1}{7^n} + \text{etc.}$$

Euler aqui estabelece, portanto, uma expressão da função zeta de Riemann (que ainda não tinha esse nome) como produto.

[4] Peter Gustav Lejeune Dirichlet (1805-1859), Alemão.

[5] **Dirichlet**, L. Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sing, unendlich viele Primzahlen erhält. **Abhandlungen der Königlich Preußischen Akademie der Wissenschaften**, p. 45–81, 1837.

[6] Bernhard Riemann (1826-1866), Alemão.

[7] **Riemann**, Bernhard. Über die Anzahl der Primzahlen unter einer gegebenen Grösse (On the Number of Primes Less Than a Given Magnitude). **Monatsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin**, p. 671–680, 1859.

Outra função relevante é a função constante um:

$$\mathbb{1}(n) = 1.$$

As três funções a seguir foram definidas e estudadas por Euler. Dessas, a função ϕ já foi definida no Capítulo 7 (Definição 7.3, na página 167).

Definição 8.3 (funções d, σ, ϕ)**.** *Para todo n positivo,*
A função $d(n)$ dá o número de divisores positivos de n;
A função $\sigma(n)$ dá a soma dos divisores positivos de n;
A função $\phi(n)$ dá o número de inteiros positivos k menores ou iguais a n, tais que $\operatorname{mdc}(k, n) = 1$. ◀

Exemplo 8.2. *Os divisores de 12 são*

$$1, 2, 3, 4, 6, 12,$$

portanto

$$\begin{aligned} d(12) &= 6, \\ \sigma(12) &= 28. \end{aligned}$$

Os números k menores que 12 tais que $\operatorname{mdc}(k, 12) = 1$ são

$$1, 5, 7, 11,$$

portanto $\phi(12) = 4$. ◀

A seguir alguns resultados básicos. O Teorema 8.1 relaciona $d(n)$ com a fatoração de n.

Teorema 8.1. *Seja n um número natural com fatoração $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$.*

$$d(n) = \prod_{i=1}^{r} (\alpha_i + 1).$$

Exemplo 8.3. *Temos $72 = 2^3 \cdot 3^2$, e os divisores de 72 são*

$$1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72,$$

portanto $d(72) = 12$. Pelo Teorema 8.1, obtemos o mesmo valor:

$$\begin{aligned} d(72) &= (3 + 1)(2 + 1) \\ &= 4 \cdot 3 \\ &= 12. \end{aligned}$$ ◀

Demonstração. Começamos observando que[8]

$$d(1) = \prod_{\emptyset} = 1$$

Agora demonstramos o Teorema por indução na quantidade de fatores primos distintos de n (cada um elevado a uma potência).
Provamos a base, com um único fator (ou seja, n é uma potência de primo p^j):

$$d(p^j) = j + 1,$$

porque $p^0, p^1, \ldots, p^j$ dividem p^j.
A hipótese de indução é que se n tem r fatores primos distintos, então

$$d(n) = \prod_{i=1}^{r} (\alpha_i + 1).$$

Agora seja $N = np^\beta$, sendo p ausente da fatoração de n ($p \nmid n$). Então, pela hipótese de indução, os divisores de N são compostos pelos $\beta + 1$ divisores de β e os $d(n)$ divisores de N:

$$\begin{aligned} c \mid N \quad &\Leftrightarrow \quad c = ab, \\ a \mid n, \quad & \quad b \mid p^\beta, \end{aligned}$$

e como $b \mid p^\beta$, b é da forma p^k, havendo $\beta + 1$ possibilidades para k (de 0 a β). A quantidade de divisores será, portanto, multiplicada por $\beta + 1$, e

$$\begin{aligned} d(N) &= (\beta + 1) \prod_{i=1}^{r} (\alpha_i + 1) \\ &= (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1)(\beta + 1). \end{aligned}$$

□

Lema 8.1. *Se p é primo, então*

$$\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1}.$$

Demonstração. Os divisores de p^k são $p^0, p^1, \ldots, p^k$. Como demonstrado no Exemplo 2.3,

$$\sum_{i=0}^{n-1} x^i = \frac{x^n - 1}{x - 1},$$

o que imediatamente nos dá o resultado, tomando $n = k + 1$. □

[8] Assim como o somatório de nenhum elemento é o neutro aditivo, $(\sum) = \sum_{\emptyset} = 0$, o produtório de nenhum elemento é o neutro multiplicativo, $(\prod) = \prod_{\emptyset} = 1$.

Teorema 8.2. *Seja n um número natural com fatoração $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Então*

$$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

Exemplo 8.4. *Seja $n = 2 \cdot 3^2 = 18$. Os divisores de 18 são*

$$1, 2, 3, 6, 9, 18,$$

cuja soma é 39. Usando a fórmula dada no Teorema 8.2,

$$\begin{aligned}
\sigma(18) &= \sigma(2 \cdot 3^2) \\
&= \left(\frac{2^{1+1} - 1}{1}\right)\left(\frac{3^{2+1} - 1}{2}\right) \\
&= \left(\frac{3}{1}\right)\left(\frac{26}{2}\right) \\
&= 39.
\end{aligned}$$

◀

Demonstração. A demonstração é por indução em quantidade de fatores primos distintos, da mesma maneira que a do Teorema 8.1, para $d(n)$. Usa-se aqui o Lema 8.1. Os detalhes são pedidos no Exercício 216. □

O Teorema 8.3 identifica uma forma fechada para ϕ; sua demonstração é o Exercício 221.

Teorema 8.3. *Se a fatoração de n é $p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, então*

$$\phi(n) = n \prod_{j=1}^{k} \left(1 - \frac{1}{p_j}\right)$$

No Teorema 8.3, os expoentes dos primos são ignorados.

Exemplo 8.5. *Calculamos $\phi(150)$. Sabemos que $150 = 2 \cdot 3 \cdot 5^2$, portanto será co-primo com todos os números que não tenham 2, 3 e 5 na fatoração. Então $\phi(150)$ é igual ao tamanho do conjunto de inteiros positivos menores que 150 divisíveis por estes números – ou, equivalentemente, 149 subtraído dos inteiros positivos que tenham 2, 3 e 5 na fatoração. Usando*[9] *o princípio*

[9] Há um método mais simples, mas só poderemos usá-lo depois de definirmos funções multiplicativas e provarmos que ϕ tem essa propriedade.

da inclusão-exclusão[10]*, concluímos que* $\phi(150)$ *é igual a*

$$\begin{aligned}
&\Big|\{n<150\ :\ 2\mid n\}\cup\{n<150\ :\ 3\mid n\}\cup\{n<150\ :\ 5\mid n\}\Big|\\
-&\Big|\{n<150\ :\ (2\cdot3)\mid n\}\cup\{n<150\ :\ (2\cdot5)\mid n\}\cup\{n<150\ :\ (3\cdot5)\mid n\}\Big|\\
+&\Big|\{n<150\ :\ (2\cdot3\cdot5)\mid n\}\Big|,
\end{aligned}$$

onde $n\in\mathbb{N}$ *e* $n>0$.
Os tamanhos dos conjuntos listados são as partes inteiras das frações

$$\frac{149}{2},\ \frac{149}{3},\ \frac{149}{5},\ \frac{149}{6},\ \frac{149}{10},\ \frac{149}{15},\ \frac{149}{30}.$$

Portanto

$$\begin{aligned}
\phi(150) &= 149-74-49-29+24+14+9-4\\
&= 40.
\end{aligned}$$

Usando o Teorema 8.3, obtemos

$$\begin{aligned}
\phi(150) &= 150\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\\
&= 150\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)\\
&= 150\cdot\frac{4}{15}\\
&= 40.
\end{aligned}$$

◀

O enunciado do Teorema 8.4 surpreende.

Teorema 8.4. *Para todo* n *positivo em* $\mathbb{Z}$*,*

O somatório é para todos os divisores d de n

$$\phi(d)\sum_{d\mid n}=n.$$

[10] O **princípio da inclusão-exclusão** trata de como determinar o tamanho de uniões de conjuntos, especialmente quando a interseção não é vazia.
$A\cup B=|A|+|B|-|A\cap B|$,
$A\cup B\cup C=|A|+|B|+|C|-|A\cap B|-|A\cap C|-|B\cap C|+|A\cap B\cap C|$,
e é generalizado como

$$\left|\bigcup_{i=1}^{n}A_i\right|=\sum_{i=1}^{n}|A_i|-\sum_{\substack{1\le i\\ <j\\ \le n}}|A_i\cap A_j|+\sum_{\substack{1\le i\\ <j\\ <k\\ \le n}}|A_i\cap A_j\cap A_k|-\cdots+(-1)^{n+1}|A_1\cap\cdots\cap A_n|.$$

Exemplo 8.6. *Os divisores de* 12 *são*

$$1, 2, 3, 4, 6, 12,$$

e então

$$\begin{aligned}\phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12) &= 1 + 1 + 2 + 2 + 2 + 4 \\ &= 12.\end{aligned}$$

◀

Demonstração. (de Gauss adaptada[11])

Ao longo da demonstração, usaremos o exemplo com $n = 6$.
Defina o conjunto

$$N = \{1, 2, \ldots, n\}.$$

Por exemplo, N poderia ser $\{1, 2, 3, \ldots, 6\}$.
Para cada divisor d de n, defina o conjunto de números que tem MDC com n igual a d:

$$N_d = \{k \in N \ : \ \mathrm{mdc}\,(k, n) = d\}.$$

Em nosso exemplo,

$$\begin{aligned} N_1 &= \{1, 5\} && (\mathrm{mdc}\,(k, 6) = 1) \\ N_2 &= \{2, 4\} && (\mathrm{mdc}\,(k, 6) = 2) \\ N_3 &= \{3\} && (\mathrm{mdc}\,(k, 6) = 3) \\ N_6 &= \{6\} && (\mathrm{mdc}\,(k, 6) = 6) \end{aligned}$$

Argumentamos que os conjuntos N_d definem uma *partição* em N – ou seja, as interseções entre eles são vazias, e a união deles é N.
Primeiro, os conjuntos N_d são disjuntos,m ou seja, se $j \neq e$, porque se $\mathrm{mdc}\,(k, n) = d$ e $\mathrm{mdc}\,(r, n) = e$, então k e r não podem estar no mesmo

[11] Gauss apresentou esta demonstração, usando a linguagem da época, no artigo 39 do *Disquisitiones.* O enunciado é

> *"Se* a, a', a'', *etc são todos os divisores de* A *(incluindo a unidade e* A*, ele mesmo), teremos*
>
> $$\phi a + \phi a' + \phi a'' + \mathrm{etc} = A."$$

Gauss dá um exemplo, com $A = 30$, e em seguida apresenta a demonstração. A título de curiosidade, esta é a forma como os conjuntos N_d são construídos no Disquisitiones (ali esse nome não lhes é dado):

> *"Multiplique por* A/a *todos os números que são primos relativos a* a *mas não maiores que* a*; faça o mesmo com* a'*, multiplicando por* A/a'*, etc. Teremos* $\phi a + \phi a' + \phi a''$ *etc números, nenhum maior que* A*."*

No resto da demonstração ele mostra que (1) os números são distintos; (2) Todos os números $1, \ldots, A$ estão incluídos, e (3) portanto o resultado segue.

Gauss, Johann Carl Friedrich. **Disquisitiones Arithmeticae**. [*S. l.*], 1801.

conjunto ($N_d \cap N_e = \emptyset$).
Além disso, os conjuntos N_d contém todos os números em N,

$$N = \bigcup_d N_d.$$

Se houvesse algum $s \in N$ tal que $s \notin N_d$ para algum divisor d, teríamos

$$\begin{aligned} &f = \operatorname{mdc}(s, n), \\ &f \mid n, \\ &s \in \{k \in N \ : \ \operatorname{mdc}(k, n) = f\}, \end{aligned}$$

uma contradição.
Em cada conjunto N_d,

i) os elementos são múltiplos de d, ou seja, são da forma rd, porque são números k com $\operatorname{mdc}(k, n) = d$;

ii) como $\operatorname{mdc}(k, n) = d$, então $\operatorname{mdc}(r, n/d) = 1$;

iii) $r \leq n/d$ (pela divisão de MDC).

Os conjuntos N_d são listados abaixo novamente, agora explicitando n/d e r.

$$\begin{aligned} N_1 &= \{1, 5\} && (d = \operatorname{mdc}(k, 6) = 1, \ \ n/d = 6, \ \ r = 1, 5) \\ N_2 &= \{2, 4\} && (d = \operatorname{mdc}(k, 6) = 2, \ \ n/d = 3, \ \ r = 1, 2) \\ N_3 &= \{3\} && (d = \operatorname{mdc}(k, 6) = 3, \ \ n/d = 2, \ \ \ r = 1) \\ N_6 &= \{6\} && (d = \operatorname{mdc}(k, 6) = 6, \ \ n/d = 1, \ \ \ r = 1) \end{aligned}$$

Os elementos em cada N_d são múltiplos de coprimos com n/d (por (ii)), e portanto sua quantidade é

$$|N_d| = \phi\left(\frac{n}{d}\right).$$

Agora,

$$\begin{aligned} |N| = n &= \sum_{d \mid n} |N_d| \\ &= \sum_{d \mid n} \phi\left(\frac{n}{d}\right) \\ &= \sum_{d \mid n} \phi(d). \end{aligned}$$

A passagem para a última linha é válida porque para cada $d \mid n$, existe exacemente um n/d, que também é divsor de n. □

Demonstração. (a de Gauss, traduzida em linguagem um pouco diferente)
Considere as n frações

$$\frac{1}{n}, \frac{2}{n}, \cdots, \frac{n}{n}.$$

Simplifique-as, deixando todas na forma reduzida.
Em todas as frações simplificadas, o demoninador será um divisor de n (se a fração era a/n e foi simplificada para b/m, evidentemente $m \mid n$). Por exemplo, quando simplificamos

$$\frac{15}{40} \longrightarrow \frac{3}{8},$$

o denominador (8) é divisor de 40.
As frações onde n ainda é o denominador são aquelas nas quais o numerador era co-primo com n. Há $\phi(n)$ destas frações.
Para cada divisor d de n haverá exatamente $\phi(d)$ frações onde o denominador é igual a d. Se somarmos todos estes $\phi(d)$ teremos o número total de frações, n. □

A demonstração acima poderá ficar mais clara com uma ilustração. Escolhemos $n = 18$ e listamos as frações. A primeira linha tem as frações antes da simplificação; a segunda as tem já simplificadas.

$$\begin{array}{cccccccccccccccccc}
\frac{1}{18} & \frac{2}{18} & \frac{3}{18} & \frac{4}{18} & \frac{5}{18} & \frac{6}{18} & \frac{7}{18} & \frac{8}{18} & \frac{9}{18} & \frac{10}{18} & \frac{11}{18} & \frac{12}{18} & \frac{13}{18} & \frac{14}{18} & \frac{15}{18} & \frac{16}{18} & \frac{17}{18} & \frac{18}{18} \\
\downarrow & & & \downarrow & & & & \downarrow & & & \downarrow & & & & \downarrow & & & \downarrow \\
\frac{1}{18} & \frac{1}{9} & \frac{1}{6} & \frac{2}{9} & \frac{5}{18} & \frac{1}{3} & \frac{7}{18} & \frac{4}{9} & \frac{1}{2} & \frac{5}{9} & \frac{11}{18} & \frac{2}{3} & \frac{13}{18} & \frac{7}{9} & \frac{5}{6} & \frac{8}{9} & \frac{17}{18} & \frac{1}{1}
\end{array}$$

Os divisores de 18 são $1, 2, 3, 6, 9$, e o número de frações com cada um deles no denominador é

$$\begin{aligned}
\phi(1) &= 1 \\
\phi(2) &= 1 \\
\phi(3) &= 2 \\
\phi(6) &= 2 \\
\phi(9) &= 6 \\
\phi(18) &= 6
\end{aligned}$$

A soma deles é 18.

8.1 Funções multiplicativas

Definição 8.4 (função (completamente) multiplicativa)**.** *Seja* f *uma função aritmética. Se, para todos inteiros* a, b *com* $\operatorname{mdc}(a, b) = 1$, $f(ab) = f(a)f(b)$,

dizemos que a função f *é* ***multiplicativa***.
Se $f(ab) = f(a)f(b)$ *mesmo quando* $\mathrm{mdc}\,(a, b) \neq 1$ *(ou seja, no caso geral), então* f *é* ***completamente multiplicativa***. ◀

Exemplo 8.7. *A função* $f(n) = n^2$ *é completamente multiplicativa, porque*

$$f(nm) = (nm)^2 = n^2 m^2 = f(n)f(m).$$ ◀

Exemplo 8.8. *A função* $f(n) = n + 1$ ***não*** *é multiplicativa:*

$$\begin{aligned} f(ab) &= ab + 1 \\ f(a)f(b) &= (a+1)(b+1) = ab + a + b + 1 \end{aligned}$$ ◀

Teorema 8.5. *Se* f *é uma função multiplicativa, então* $f(1) = 1$.

Demonstração. Seja n tal que $f(n) \neq 0$. Então $f(n) = f(n \cdot 1) = f(n)f(1)$, o que implica que $f(1) = 1$. □

Teorema 8.6. *As funções* ϕ, σ, d *são multiplicativas.*

Exemplo 8.9. $\mathrm{mdc}\,(6, 5) = 1$*, e os valores de* ϕ, σ *e* d *para os dois números são*

$$\begin{aligned} \phi(6) &= 2, & \phi(5) &= 4, \\ d(6) &= 4, & d(5) &= 2, \\ \sigma(6) &= 12, & \sigma(5) &= 6. \end{aligned}$$

Como as funções são multiplicativas, temos

$$\begin{aligned} \phi(30) &= \phi(6 \cdot 5) \\ &= \phi(6)\phi(5) \\ &= 2 \cdot 4 \\ &= 8. \end{aligned}$$

E de fato, há 8 números cujo MDC com 30 é um:

$$1, 7, 11, 13, 17, 19, 23, 29.$$

Verificamos os divisores.

$$\begin{aligned} d(30) &= d(6 \cdot 5) \\ &= d(6)d(5) \\ &= 4 \cdot 2 \\ &= 8. \end{aligned}$$

E são oito os divisores de 30:

$$1, 2, 3, 5, 6, 10, 15, 30.$$

Quanto à função σ,

$$\begin{aligned}\sigma(30) &= \sigma(6 \cdot 5)\\ &= \sigma(6)\sigma(5)\\ &= 12 \cdot 6\\ &= 72,\end{aligned}$$

que é a soma dos divisores de 30. ◀

Demonstração. Sejam $a, b \in \mathbb{Z}$, com $\operatorname{mdc}(a, b) = 1$. Suponha que as fatorações de a e b sejam

$$\begin{aligned}a &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}\\ b &= q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s},\end{aligned}$$

onde não há $p_i = q_j$. Qualquer divisor de ab será representado de maneira única como produto de divisores de ab:

$$d \mid ab \;\Rightarrow\; d = \prod_{\substack{i \le r\\ j \le s}} p^{\gamma_i} q^{\delta_j}.$$

Claramente, se há A divisores de a e B divisores de b, e a interseção dos dois conjuntos de divisores é vazia (porque a e b não tem primos em comum), então a quantidade $d(ab)$ é igual ao produto das quantidades $d(a)$ e $d(b)$,

$$d(ab) = d(a)d(b).$$

Para σ, temos

$$\begin{aligned}\sigma(ab) = \sum_{d \mid ab} d &= \left(\sum_{s \mid a} s\right)\left(\sum_{t \mid b} t\right)\\ &= \sigma(a)\sigma(b).\end{aligned}$$

Para ϕ, observe os anéis $\mathbb{Z}_a$, $\mathbb{Z}_b$ e $\mathbb{Z}_{ab}$. Pelo Teorema Chinês dos Restos, a função $f : \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$,

$$f(x) = (x, x),$$

é bijetora.
(x, x) é unidade se e somente se x é unidade em $\mathbb{Z}_a$ e em $\mathbb{Z}_b$, o que significa que $x \pmod{ab}$ é unidade se e somente se $x \pmod{a}$ e $x \pmod{b}$ são

unidades.
Mas a quantidade de unidades em $\mathbb{Z}_n$ é igual a $\phi(n)$, logo, a quantidade de unidades em $\mathbb{Z}_{ab}$ é igual ao produto das quantidades de unidades em $\mathbb{Z}_a$ e $\mathbb{Z}_b$.

$$\phi(ab) = \phi(a)\phi(b). \qquad \square$$

Usando a multiplicidade de ϕ, podemos construir uma demonstração diferente para o Teorema 8.4.

Demonstração. (do Teorema 8.4, usando multiplicidade de ϕ) Temos duas funções multiplicativas,

$$f(n) = \sum_{d|n} \phi(n)$$
$$g(n) = n$$

A multiplicidade de f é simples de verificar, usando a multiplicidade de ϕ.
Dessa forma, se mostrarmos que $f(p^a) = p^a$, pela multiplicidade de f e g, teremos o resultado desejado.
Usaremos um fato simples (a demonstração é pedida no Exercício 212):

$$\phi(p^a) = p^a - p^{a-1}.$$

Agora temos

$$\begin{aligned} f(p^a) = \sum_{d|p^a} \phi(p^a) &= \sum_{i=0}^{a} \phi(p^i) \\ &= 1 + \sum_{i=1}^{a} \phi(p^i) \\ &= 1 + \sum_{i=1}^{a} p^i - p^{i-1} \\ &= p^a, \end{aligned}$$

como queríamos demonstrar. $\square$

8.2 Números Perfeitos

Números perfeitos foram definidos no Capítulo 5. Reproduzimos aqui a definição:

Definição 8.5 (número perfeito)**.** *n é um **número perfeito** se é igual à soma de seus divisores próprios.* ◀

Naquele capítulo, provamos o Teorema 5.4[12] que determina que se $2^p - 1$ é um primo de Mersenne, então $(2^p - 1)2^{p-1}$ é perfeito. Agora provamos outra relação entre números perfeitos e primos de Mersenne, e desta vez usamos a multiplicidade de σ na demonstração.

Teorema 8.7. *Todo número perfeito par pode ser escrito na forma* $2^{n-1}(2^n - 1)$*, onde* $2^n - 1$ *é primo de Mersenne.*

Demonstração. Seja $m = 2^{n-1}k$ um número perfeito, com k ímpar. Emtão $\mathrm{mdc}\left(k, 2^{n-1}\right) = 1$. Com isso, usamos o fato de σ ser multiplicativa:

$$\begin{aligned}\sigma(m) &= \sigma(2^{n-1}k)\\ &= \sigma(2^{n-1})\sigma(k)\\ &= \left(\frac{2^{n-1}}{2-1}\right)\sigma(k)\\ &= (2^n - 1)\sigma(k). \end{aligned} \tag{8.1}$$

Como m é perfeito,

$$\begin{aligned}\sigma(m) &= 2m\\ &= 2^n k. \end{aligned} \tag{8.2}$$

Combinamos 8.1 e 8.2:

$$k = \frac{(2^n - 1)\sigma(k)}{2^n}. \tag{8.3}$$

Como $2^n \nmid 2^n - 1$ e $k \in \mathbb{Z}$, então $2^n \mid \sigma(k)$: existe r tal que

$$\sigma(k) = r2^n. \tag{8.4}$$

Combinamos agora 8.2 e 8.4:

$$k = (2^n - 1)r.$$

Suponha que $r = 1$. Então $k = 2^n - 1$. Como $\sigma(k) = 2^n$ quando $r = 1$, então necessariamente $\sigma(m) = m + 1$ e m é primo (a soma dos divisores de um primo é ele mais um).

Agora suponha $r > 1$. Então temos, como divisores de k, ao menos $1, r, 2^n - 1$ e $(2^n - 1)r$. Por isso,

$$\begin{aligned}\sigma(k) &> 1 + q + 2^n - 1 + (2^n - 1)r\\ &= 2^n(r + 1).\end{aligned}$$

[12] **Teorema 5.4:** Seja $2^p - 1$ um primo de Mersenne. Então $(2^p - 1)2^{p-1}$ é perfeito.

Dividindo k por $\sigma(k)$, obtemos

$$\begin{aligned}\frac{k}{\sigma k} &\leq \frac{(2^n-1)r}{2^n(r+1)}\\ &= \left(\frac{2^n-1}{2^n}\right)\left(\frac{q}{q+1}\right)\\ &< \frac{2^{n-1}}{2^n}.\end{aligned}$$

Mas isto contradiz , portanto $r = 1$ e $2^n - 1$ é primo de Mersenne. □

8.3 Convolução de Dirichlet

A convolução de Dirichlet é uma forma de combinar funções.

Definição 8.6 (convolução de Dirichlet)**.** *Se* f, g *são duas funções aritméticas, a* ***convolução de Dirichlet*** *de* f *com* g*, denotada* $f * g$*, é*

$$(f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right).$$ ◀

O que a convolução de Dirichlet faz[13] é combinar os divisores do argumento n, aplicando f em um e g em outro. Por exemplo, suponha que f e g são funções aritméticas, e considere o argumento $n = 18$. Os divisores de 18 são

$$1, 2, 3, 6, 9, 18.$$

A convolução de f e g (quaisquer que sejam) nos dará

$$\begin{aligned}(f * g)(18) = f(1)g(18) + f(2)g(9) + f(3)g(6)\\ + f(6)g(3) \ \ + f(9)g(2) + f(18)g(1).\end{aligned}$$

Definição 8.7 (inversa de função aritmética)**.** *Se* f *é uma função aritmética, então a* ***inversa*** *de* f*, se existir, é a função artmética* g *tal que* $f * g = \delta$*.* ◀

[13] No corpo do texto, é a exposição mais intuitiva que podemos dar. Aqui, em nota de rodapé, fazemos mais! A **série de Dirichlet** de f é

$$D(f, s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s},$$

e a convolução de Dirichlet de duas funções é a convolução das séries de Dirichlet delas:

$$D(f * g, s) = D(f, s)D(g, s).$$

Exemplo 8.10. *A inversa de δ é ela mesma.*

$$(\delta * \delta)(n) = \sum_{d|n} \delta(d)\delta\left(\frac{n}{d}\right).$$

Quando $n = 1$,

$$\begin{aligned}(\delta * \delta)(1) &= \sum_{d|1} \delta(d)\delta\left(\frac{1}{d}\right) \\ &= \delta(1)\left(\frac{1}{1}\right) \\ &= 1.\end{aligned}$$

Quando $n > 1$,

$$\begin{aligned}(\delta * \delta)(n) &= \sum_{d|n} \underbrace{\delta(d)}_{\substack{\text{nulo} \\ \text{para } d>1}} \underbrace{\delta\left(\frac{n}{d}\right)}_{\substack{\text{nulo} \\ \text{para } d<n}} \\ &= 0.\end{aligned}$$

◀

Teorema 8.8. *Uma função aritmética f tem inversa se e somente se $f(1) \neq 0$.*

Demonstração. A demonstração é por indução forte em n.
Para $n = 1$ há um único divisor, o próprio um. Então, para qualquer função g,

$$\begin{aligned}(f * g)(1) &= \sum_{d|1} f(d)g\left(\frac{1}{d}\right) \\ &= f(1)g\left(\frac{1}{1}\right) \\ &= f(1)g(1).\end{aligned}$$

Para que g seja inversa de f, precisamos que o valor $(f * g)(1)$ seja igual a $\delta(1) = 1$:

$$\begin{aligned}f(1)g(1) &= 1 \\ g(1) &= \frac{1}{f(1)},\end{aligned}$$

o que claramente só é possível se $f(1) \neq 0$.
Para $n > 1$, suponha que o enunciado vale para todo $k < n$. Podemos então construir g a partir de f. Assim, sendo $n > 1$, $\delta(n) = 0$, e

$$(f * g)(n) = 0 = \sum_{d|n} f(d)g\left(\frac{n}{d}\right)$$
$$0 = f(1)g(n) + \sum_{\substack{d|n \\ d<n}} f(d)g\left(\frac{n}{d}\right)$$
$$g(n) = -\frac{1}{f(1)} \sum_{\substack{d|n \\ d<n}} f(d)g\left(\frac{n}{d}\right)$$

Nesta última fórmula, $f(1) \neq 0$, portanto podemos calcular $-1/f(1)$. Além disso, dentro do somatório somente usamos g aplicada aos divisores d estritamente menores que n, que pela hipótese de indução existem, e como são divisores de n, não são zero.
A demonstração indutiva também resulta em um método recursivo para determinar a inversa g. □

Teorema 8.9. *As funções aritméticas, quando consideradas com a operação usual de soma de funções, e a operação de convolução de Dirichlet, formam um anel comutativo e associativo com unidade.*

Corolário 8.1. *O inverso de uma função aritmética, se existir, é único.*

Demonstração. Segue diretamente do Teorema 8.9 (as funções aritméticas formam um anel) e 2.11 (o inverso em um anel é único). □

A função μ de Möbius[14] é definida de forma a caracterizar quando um número é livre de quadrados. Sua importância está também em outros fatos. Por exemplo, suponha que para duas funções aritméticas quaisquer, f e g, sempre seja verdade que

$$f(n) = \sum_{d|n} g(d).$$

[14] Esta função era usada, implicitamente (sem um "nome") nos trabalhos de diversos matemáticos. Hardy e Wright mencionam que

> $\mu(n)$ *ocorre implicitamente nos trabalhos de Euler tão cedo quanto 1748, mas Möbius, em 1832, foi o primeiro a investigar suas propriedades sistematicamente.*

No original,

> $\mu(n)$ *occurs implicitly in the works of Euler as early as 1748, but Möbius, in 1832, was the first to investigate its properties systematically.*

Hardy, G. H.; **Wright**, E. M. **An Introduction to The Theory of Numbers**. 6. ed. [*S. l.*]: Oxford, 2009.

O comentário está no final do Capítulo XVI, na seção de notas.
Em 1832 August Ferdinand Möbius publicou um estudo com a definição da função, que é extensamente usada em teoria analítica de números, sendo também útil em Combinatória. Gauss encontrou uma definição alternativa, usando o conceito de *raiz primitiva*, e é enunciada (Teorema 8.15), com demonstração pedida como Exercício (número 240) no Capítulo 7.

A fórmula da inversão de Moebius dá uma forma fechada para a expressão de g em função de f.

Definição 8.8 (função μ, de Moebius)**.** *Seja $n \in \mathbb{Z}$. A **função μ de Moebius** é a função multiplicativa tal que*

$$\begin{aligned} \mu(1) &= +1, \\ \mu(p) &= -1, \\ \mu(p^2) &= 0. \end{aligned}$$

◀

Tratamos 1 separadamente na definição porque não é primo.
Como exigimos na Definição 8.8 que μ seja multiplicativa, observamos que que pode ser interessante usar a Definição 8.9 para μ. Note que a primeir adefinição implica trivialmente nas propriedades descritas na segunda, por exigir que μ seja multiplicativa – mas a que a segunda definição implica na multiplicatividade não é trivial, e o demonstramos adiante (Teorema 8.10).

Definição 8.9 (função μ, de Moebius - segunda definição)**.** *Seja $n \in \mathbb{Z}$. A **função μ de Moebius** é*

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1, \\ 0 & \text{se } p^2 \mid n \ \ (p \text{ primo}), \\ (-1)^k & \text{se } n = p_1 p_2 \dots p_k \ \ (p_i \neq p_j). \end{cases}$$

◀

Exemplo 8.11.

$$\begin{aligned} \mu(7) = (-1)^1 &= -1 \\ \mu(21) = \mu(3 \cdot 7) = (-1)^2 &= +1 \\ \mu(30) = \mu(2 \cdot 3 \cdot 5) = (-1)^3 &= -1 \\ \mu(60) = \mu(2^2 \cdot 3 \cdot 5) &= \ \ 0 \end{aligned}$$

◀

Teorema 8.10. *A Definição 8.9, embora não o explicite, implica na propriedade da multiplicatividade de μ, sendo portanto equivalente à Definição 8.8.*

Demonstração. Sejam

$$\begin{aligned} a &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} \\ b &= q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t} \end{aligned}$$

Presumimos que não há fator comum, já que a definição de função multiplicativa só trata de casos em que $\operatorname{mdc}(a, b) = 1$.

Suponha que todos os α_i e β_j são iguais a um (a e b são ambos livres de quadrado). Então

$$\begin{aligned}\mu(a) &= (-1)^s \\ \mu(b) &= (-1)^t,\end{aligned}$$

e como a e b não tem primos em comum em sua fatoração, ab será também livre de quadrado, e

$$\mu(ab) = (-1)^{s+t} = \mu(a)\mu(b).$$

Agora, sem perda de generalidade, suponha que a não é livre de quadrado: um dos α_i é maior que um. Então $\mu(a) = 0$. Mas se a tem um fator primo elevado a potência maior que um, ab também tem. Assim,

$$\mu(ab) = 0 = \mu(a)\mu(b).$$

Finalmente, se $a = 1$, então

$$\begin{aligned}\mu(ab) &= \mu(1 \cdot b) \\ &= \mu(b) \\ &= 1 \cdot \mu(b) \\ &= \mu(a)\mu(b).\end{aligned}$$

e terminamos de verificar todos os casos. □

Teorema 8.11. *Para todo inteiro positivo n,*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{se } n = 1, \\ 0 & \text{se } n > 1. \end{cases}$$

Exemplo 8.12. *Os divisores de 6 são $1, 2, 3, 6$, portanto*

$$\begin{aligned}\mu(1) &= +1 \\ \mu(2) &= (-1)^1 = -1 \\ \mu(3) &= (-1)^1 = -1 \\ \mu(6) &= \mu(2 \cdot 3) = (-1)^2 = +1\end{aligned}$$

Temos então

$$\begin{aligned}\sum_{d|6}\mu(d) &= \mu(1)+\mu(2)+\mu(3)+\mu(6)\\ &= (+1)+(-1)+(-1)+(+1)\\ &= 0.\end{aligned}$$

◀

Demonstração. Esta demonstração é realizada em três casos. Um caso para $n = 1$, um caso para n decomposto em um único primo (ou seja, n é potência de primo) e outro para n tendo vários primos diferentes na fatoração. Embora a divisão em casos seja parecida com a que faríamos em uma demonstração por indução, a demonstração é direta.

Primeiro, a fórmula está correta para $n = 1$ porque

$$\sum_{d|1} d = 1.$$

Verificamos agora que a fórmula está correta para um único primo p, de forma que $n = p^a$. Como os divisores de p^a são $p^0, p^1, \ldots, p^a$, então

$$\begin{aligned}\sum_{d|p^a}\mu(p^a) &= \mu(1)+\mu(p)+\mu(p^2)+\mu(p^3)+\cdots+\mu(p^a)\\ &= 1-1+0+0+\cdots+0\\ &= 0.\end{aligned}$$

Agora tratamos do segundo caso, em que $n = mp^a$, onde m tem k divisores primos, e que p é primo (simplesmente separamos um dos primos p da fatoração de n).

$$\begin{aligned}\sum_{d|n}\mu(d) &= \overbrace{\sum_{d|m}\mu(d)}^{d|mp^0}+\overbrace{\sum_{d|m}\mu(pd)}^{d|mp^1}+\overbrace{\sum_{d|m}\mu(p^2d)}^{d|mp^2}+\cdots+\overbrace{\sum_{d|m}\mu(p^ad)}^{d|mp^a}\\ &= \sum_{d|m}\mu(d)+\sum_{d|m}\mu(p)\mu(d)+0+0+\cdots+0\\ &= \sum_{d|m}\mu(d)+\sum_{d|m}(-1)\mu(d)+0+0+\cdots+0\\ &= \sum_{d|m}\mu(d)-\sum_{d|m}\mu(d)+0+0+\cdots+0\\ &= 0.\end{aligned}$$

□

Teorema 8.12 (fórmula da inversão de Moebius)**.** *Sejam f, g funções aritméticas, não necessariamente multiplicativas. Então, as duas afirmações a*

seguir são equivalentes.

$$\forall n \in \mathbb{Z}, \quad f(n) = \sum_{d|n} g(d) \tag{8.5}$$

$$\forall n \in \mathbb{Z}, \quad g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right) \tag{8.6}$$

Dizemos que as funções f *e* g *são um* par de Moebius.

Uma maneira alternativa de escrever a Equação 8.6 é

$$\forall n \in \mathbb{Z}, \quad g(n) = \sum_{ab=n} \mu(a) f(b).$$

Exemplo 8.13. *Já sabemos, pelo Teorema 8.4, que*

$$n = \sum_{d|n} \phi(d).$$

Isto é o mesmo que determinar $f(n) = n$*, e escrever*

$$f(n) = \sum_{d|n} \phi(d).$$

A fórmula de inversão de Moebius determina, portanto, que

$$\begin{aligned} \phi(n) &= \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) \\ &= \sum_{d|n} \mu(d) \left(\frac{n}{d}\right) \\ &= n \sum_{d|n} \frac{\mu(d)}{d}. \end{aligned}$$

Para exemplificar, calculamos $\phi(540)$ *de duas maneiras. Primeiro, usamos a definição de* $\phi(n)$*, e o fato de ser multiplicativa.*

$$\begin{aligned} \phi(540) &= \phi(2^2 \cdot 3^3 \cdot 5) \\ &= \phi(2^2) \cdot \phi(3^3) \cdot \phi(5) \\ &= 2 \cdot 18 \cdot 4 \\ &= 144. \end{aligned}$$

Agora usamos a fórmula que obtivemos usando a inversão de Moebius (apenas como ilustração do conceito, porque neste caso nos será mais trabalhoso

do que calcular $\phi(n)$ usando a definição como fizemos):

$$\phi(540) = 540 \sum_{d|540} \frac{\mu(d)}{d}.$$

Observamos que $540 = 2^2 \cdot 3^3 \cdot 5$, *mas* $\mu(2^2) = \mu(3^2) = \mu(3^3) = 0$, *porque todos tem fatores primos repetidos. Não precisamos, assim, considerar os termos em que estes aparecem.*

$$\phi(540) = 540\Big(\cdots + \underbrace{\frac{\mu(2^2)}{2^2}}_{\substack{=0/2^2 \\ =0}} + \cdots \Big)$$

Podemos então usar apenas os divisores 1, 2, 3, 5, $2\cdot 3$, $2\cdot 5$, $3\cdot 5$ *e* $2\cdot 3\cdot 5$. *Calculamos:*

$$\begin{aligned}
\phi(540) &= 540 \sum_{D|540} \frac{\mu(D)}{D} && \text{(D livre de quadrados)} \\
&= 540 \left(\frac{\mu(1)}{1} + \frac{\mu(2)}{2} + \frac{\mu(3)}{3} + \frac{\mu(5)}{5} + \right. \\
&\qquad \left. \frac{\mu(2\cdot 3)}{2\cdot 3} + \frac{\mu(2\cdot 5)}{2\cdot 5} + \frac{\mu(3\cdot 5)}{3\cdot 5} + \frac{\mu(2\cdot 3\cdot 5)}{2\cdot 3\cdot 5} \right) \\
&= 540 \left[+1 - 1\left(\frac{1}{2}\right) - 1\left(\frac{1}{3}\right) - 1\left(\frac{1}{5}\right) \right. \\
&\qquad \left. +1\left(\frac{1}{2\cdot 3}\right) + 1\left(\frac{1}{2\cdot 5}\right) + 1\left(\frac{1}{3\cdot 5}\right) - 1\left(\frac{1}{2\cdot 3\cdot 5}\right) \right] \\
&= 540 - 270 - 180 - 108 + 90 + 54 + 36 - 18 \\
&= 144. && \blacktriangleleft
\end{aligned}$$

Demonstração. Tratamos das duas implicações separadamente. Começamos com (8.5 $\Rightarrow$ 8.6).

Sejam então f e g duas funções aritméticas, e presuma que 8.5 vale.

$$\begin{aligned}
\sum_{ab=n} \mu(a) f(b) &= \sum_{ab=n} \left[\mu(a) \sum_{d|b} g(d) \right] && \text{(por 8.5)} \\
&= \sum_{ad|n} \mu(a) g(d) \\
&= \sum_{d|n} g(d) \sum_{a|\frac{n}{d}} \mu(a)
\end{aligned}$$

Mas pelo Teorema 8.11,

$$\sum_{d|\frac{n}{d}} \mu(d) = \begin{cases} 1 & \text{se } n/d > 1, n > d \\ 0 & \text{se } n/d = 1, n = d. \end{cases}$$

e na última equação,

$$\sum_{a|n} \mu(a) g\left(\frac{n}{d}\right) = \sum_{a|n} g(a) \sum_{d|\frac{n}{d}} \mu(a),$$

temos $\sum_{a|\frac{n}{d}} \mu(d)$ igual a zero quando $n/d > 1$,
e igual a um quanto $n = d$, portanto

$$\begin{aligned} \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) &= \sum_{n|n} g(n) \\ &= g(n), \end{aligned}$$

e, partindo de 8.5, $f(n) = \sum_{d|n} g(d)$, determinamos que

$$g(n) = \sum_{ab=n} \mu(a) f(b).$$

Como presumimos (8.5) neste desenvolvimento, ele só estabelece que (8.5) implica em (8.6). Precisamos estabelecer o outro sentido da implicação.

Passamos agora a demonstrar (8.6 $\Rightarrow$ 8.5). Novamente, presuma que f e g são funções aritméticas, e presuma que 8.6 vale.

$$\begin{aligned} \sum_{a|n} g(a) &= \sum_{a|n} \mu(a) \sum_{d|a} f\left(\frac{a}{d}\right) && \text{(por (8.6))} \\ &= \sum_{a|n} \sum_{d|a} \mu(a) f\left(\frac{a}{d}\right) \\ &= \sum_{a|n} \sum_{d|a} f(a) \mu\left(\frac{a}{d}\right) \\ &= \sum_{a|n} f(a) \left(\sum_{d|a} \mu\left(\frac{a}{d}\right) \right) \end{aligned}$$

Novamente, $\sum_{d|a} \mu\left(\frac{a}{d}\right)$ é zero quando $a/d > 1$ e um quando $a = d$:

$$\begin{aligned}\sum_{a|n} f(a)\left(\sum_{d|a} \mu\left(\frac{a}{d}\right)\right) &= f(n)(1) + \sum_{\substack{d|a \\ d<a}} f(n)(0) \\ &= f(n).\end{aligned}$$

Estabelecemos, portanto, que $f(n) = \sum_{a|n} g(a)$ (8.5), usando (8.6). □

Exemplo 8.14. *Alguns exemplos de pares de Moebius são*

$$\begin{aligned}(n, \phi(n)) :&\ n = \sum_{d|n} \phi(d) \\ (d(n), 1) :&\ d(n) = \sum_{d|n} 1 \\ (\sigma(n), id) :&\ \sigma(n) = \sum_{d|n} d\end{aligned}$$ ◀

Teorema 8.13. *Se f, g é um par de Moebius, e uma delas é multiplicativa, então a outra também é.*

Demonstração. Suponha que f e g sejam um par de Moebius,

$$\begin{aligned}\forall n \in \mathbb{Z},\ \ f(n) &= \sum_{d|n} g(d) \\ \forall n \in \mathbb{Z},\ \ g(n) &= \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right)\end{aligned}$$

e que $\mathrm{mdc}\,(a, b) = 1$. Então, se g é multiplicativa,

$$\begin{aligned}f(ab) &= \sum_{d|ab} g(d) \\ &= \sum_{c|a}\sum_{e|b} g(ce) && (\mathrm{mdc}\,(a,b) = 1) \\ &= \sum_{c|a}\sum_{e|b} g(c)g(e) && (g \text{ é multiplicativa}) \\ &= \sum_{c|a} g(c) \sum_{e|b} g(e) \\ &= f(a)f(b).\end{aligned}$$

Se f é multiplicativa,

$$\begin{aligned}
g(ab) &= \sum_{d|ab} \mu(d) f\left(\frac{ab}{d}\right) \\
&= \sum_{c|a} \sum_{e|b} \mu(ce) f\left(\frac{ab}{ce}\right) && (\mathrm{mdc}\,(a,b) = 1) \\
&= \sum_{c|a} \sum_{e|b} \mu(c)\mu(e) f\left(\frac{a}{c}\right) f\left(\frac{b}{e}\right) && (f, \mu \text{ multiplicativas}) \\
&= \sum_{c|a} \mu(c) f\left(\frac{a}{c}\right) \sum_{e|b} \mu(e) f\left(\frac{b}{e}\right) \\
&= g(a)g(b). && \square
\end{aligned}$$

Os Teoremas 8.15 e 8.14 estabelecem formas fechadas para a soma e o produto das n-ésimas raízes primitivas da unidade (as demonstrações são pedidas nos Exercícios 239 e 240).

Teorema 8.14. *Se $n > 2$, o produto das n-ésimas raízes primitivas da unidade é um.*

Teorema 8.15. *A soma das n-ésimas raízes primitivas da unidade é $\mu(n)$, onde μ é a função de Möebius.*

8.4 Função de Mangoldt, $\Lambda(x)$

A função de von Mangoldt é relevante no estudo da distribuição dos números primos. O nome da função é homenagem a von Mangoldt[15]. Neste contexto, é interessante como exemplo de função que não é multiplicativa nem aditiva, e para uma interessante aplicação da inversão de Möbius.

Definição 8.10 (função de Mangoldt)**.** *Para todo inteiro positivo n, a **função de Mangoldt** é*

$$\Lambda(x) = \begin{cases} \log p & \text{se } n = p^m \text{ para algum } m, \text{ e} \\ 0 & \text{caso contrário.} \end{cases} \qquad \blacktriangleleft$$

Exemplo 8.15. *A tabela a seguir mostra os valores de $\Lambda(n)$, para $1 \leq n \leq 12$.*

n :	1	2	3	4	5	6	7	8	9	10	11	12
$\Lambda(n)$:	0	$\log 2$	$\log 3$	$\log 2$	$\log 5$	0	$\log 7$	$\log 2$	$\log 3$	0	$\log 11$	0

A função não é definida em $n = 0$. $\blacktriangleleft$

[15] Hans Carl Friedrich von Mangoldt (1854-1925), Alemão.

Teorema 8.16. *A função de Mangoldt não é multiplicativa.*

Teorema 8.17. *Para todo* $n > 1$*,*

$$\sum_{d|n} \Lambda(d) = \log(n).$$

Demonstração. A fatoraçào de n é

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Então cada divisor de n é (i) potência de um único primo ou (ii) compostos por mais de um primo. No somatório

$$\sum_{d|n} \Lambda(d)$$

somente os do tipo (i) contribuem, e cada primo p_i na fatoração contribui $alpha_i$ vezes com $\log(p_i)$:

$$\begin{aligned} p &\mid n \\ p^2 &\mid n \\ &\vdots \\ p^{\alpha_i} &\mid n \end{aligned}$$

E cada uma dessas vezes, a contribuição é de $\log(p_i)$ (*sem* o expoente). Assim, o divisor $p_i^{\alpha_i}$ soma

$$\underbrace{\log(p_i) + \log(p_i) + \cdots + \log(p_i)}_{\alpha_i \text{ vezes}} = \alpha_i \log(p_i).$$

O somatório é, portanto,

$$\begin{aligned} \sum_{d|n} \Lambda(d) &= \sum_{i=1}^{k} \alpha_i \log(p_i) \\ &= \log\left(\prod_i p_i^{\alpha_i}\right) \\ &= \log(n). \end{aligned}$$

□

Exemplo 8.16. *Para* $n = 18$,

$$\begin{aligned}\sum_{d|15} \Lambda(d) &= \Lambda(1) + \Lambda(2) + \Lambda(3) + \Lambda(6) + \Lambda(9) + \Lambda(18) \\ &= 0 + \log(2) + \log(3) + 0 + \log(3) + 0 \\ &= \log(2 \cdot 3 \cdot 3) \\ &= \log(18).\end{aligned}$$

◀

Teorema 8.18.

$$\Lambda(n) = \sum_{d|n} \mu \log\left(\frac{n}{d}\right) = -\sum_{d|n} \mu(d)\log(d)$$

Demonstração. Usando a inversão de Möbius no enunciado do Teorema 8.17,

$$\begin{aligned}\sum_{d|n} \Lambda(d) &= \log(n) \\ \Lambda(n) &= \sum_{d|n} \mu(d)\log\left(\frac{n}{d}\right) && \text{(inv. de Möbius)} \\ &= \sum_{d|n} (\mu(d)\log(n) - \log(d)) \\ &= \underbrace{\log(n)\sum_{d|n} \mu(d)}_{(*)} - \sum_{d|n} \mu(d)\log(d)\end{aligned}$$

Em $(*)$, temos que quando $n = 1$, $\log(n) = 0$; e quando $n > 1$, $\sum_{d|n} \mu(d) = 0$, portanto

$$\Lambda(n) = -\sum_{d|n} \mu(d)\log(d).$$

□

8.5 Maior Inteiro (chão), $\lfloor x \rfloor$

A noção natural de "número inteiro menor que ou igual a x" é de uso suficiente amplo para que tenham sido definidas para ela nome e notação.

Definição 8.11 (menor inteiro maior ou igual a x (chão de x))**.** *Se* $x \in \mathbb{R}$*, o* ***maior inteiro menor ou igual a*** x*, ou* ***chão de*** x*, é denotado por* $\lfloor x \rfloor$ *ou* $[x]$*. O conceito simétrico é o de* ***menor inteiro maior ou igual a*** x*, ou* ***teto de*** x*, denotado* $\lceil x \rceil$*.* ◀

Esta não é uma função aritmética, porque o domínio é $\mathbb{R}$ e o contradomínio é $\mathbb{Z}$, mas é tracionalmente estudada no mesmo contexto.

Exemplo 8.17.

$$\begin{array}{rr} \lfloor 0 \rfloor = 0 & \lfloor e \rfloor = 2 \\ \lfloor 1/2 \rfloor = 0 & \lfloor \varphi \rfloor = 1 \\ \lfloor 3/2 \rfloor = 1 & \left\lfloor \sqrt{2} \right\rfloor = 1 \\ \lfloor -1/2 \rfloor = -1 & \left\lfloor -\sqrt{2} \right\rfloor = -2 \\ \lfloor -3/2 \rfloor = -2 & \\ \lfloor 3 \rfloor = 3 & \lfloor \pi \rfloor = 3 \end{array}$$

◀

Exemplo 8.18. *O número de dígitos necessário para representar um número* n *em base dez é*

$$\lfloor \log_{10}(n) \rfloor + 1.$$

De maneira geral, o número de dígitos necessário para representar um número n *em base* b *é*

$$\lfloor \log_b(n) \rfloor + 1.$$ ◀

Por ser simétrico a $\lfloor x \rfloor$, não trataremos de $\lceil x \rceil$. O Teorema 8.19 lista algumas propriedades de $\lfloor x \rfloor$, que são de simples verificação.

Teorema 8.19. *Para todos* $x, y \in \mathbb{R}$, $n \in \mathbb{Z}$,

(a) $x = \lfloor x \rfloor + f$, *onde* $f \in [0, 1)$ *é a* parte fracionária *de* x.

(b) $\lfloor x + n \rfloor = \lfloor x \rfloor + n$.

(c) $\lfloor x \rfloor + \lfloor -x \rfloor$ *é zero se* $x \in \mathbb{Z}$, *senão é* -1.

(d) $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor$.

(e) $\lfloor x/n \rfloor = \lfloor \lfloor x \rfloor / n \rfloor$, *se* $n > 0$.

(f) $0 \leq \lfloor x \rfloor - 2 \lfloor x/2 \rfloor \leq 1$.

(g) $| \mathbb{Z} \cap (x, y] | \; = \; \lfloor y \rfloor - \lfloor x \rfloor$.

(h) $| \{kn : k \in \mathbb{Z}^+, kn \leq x\} | = \lfloor x/n \rfloor$

(i) *O menor inteiro congruente a* $n \mod m$ *é o* $k \in \mathbb{Z}$ *tal que* $n = m \lfloor a/m \rfloor + k$.

No Teorema 8.20, que traz a fórmula de de Polignac-Legendre [16], afirmamos que há uma forma fechada simples para a ordem do expoente de um

[16] O primeiro nome é "Alfonse de Polignac", daí o duplo "de". O mesmo ocorre com os Teoremas de De Morgan em Lógica.

primo na fatoração de $n!$ – ou seja, podemos facilmente saber qual a maior potência de um primo p que divide $n!$.

Teorema 8.20 (fórmula de de Polignac e Legendre)**.** *Sejam p primo e n inteiro positivo. Então*

$$\operatorname{ord}_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

Exemplo 8.19. *Por exemplo, se $p = 7$ e $n = 20$, temos*

$$\begin{aligned}
\operatorname{ord}_7(20!) &= \sum_{i=1}^{\infty} \left\lfloor \frac{20}{7^i} \right\rfloor \\
&= \left\lfloor \frac{20}{7} \right\rfloor + \left\lfloor \frac{20}{7^2} \right\rfloor + \cdots \\
&= \lfloor 2.857\cdots \rfloor + \lfloor 0.408\cdots \rfloor + \cdots \\
&= 2 + 0 + \cdots \\
&= 2,
\end{aligned}$$

porque os termos mais adiante são todos zero. E a ordem de 7 em 20! é, de fato, dois:

$$20! = 2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19.$$ ◀

Demonstração. A soma sempre é finita, porque quando $p^i > n$, $\lfloor n/p^i \rfloor = 0$. Claramente, os únicos primos que dividem $n!$ são menores ou iguais que n. O último deles é $\lfloor n/p \rfloor$.
Se visualizarmos $n!$ como produto de inteiros, cada um com sua fatoração única, teremos

$$n! = 1 \cdot 2 \cdot \cdots (p_1 p_2 \ldots p_k) \cdots (n-1)n,$$

Cada fator em $n!$ contribui com algum p^j. Se dividirmos n por p, estaremos contando o número de vezes que p aparece com expoente ≥ 1 em $n!$. Ao dividirmos por p^2, o número de vezes que aparece com expoente ≥ 2, e assim por diante.
Assim, a soma

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots$$

contabiliza exatamente a soma dos expoentes de p em $n!$. □

O Exemplo 8.20 é uma interessante aplicação do Teorema 8.20.

Exemplo 8.20. *Provaremos que o número*

$$\frac{100!}{(10!)^{10} 11!}$$

é inteiro.

Precisamos mostrar que, para cada potência de primo p^r *na fatoração do denominador, existe um fator* p^s *no numerador, com* $s \geq b$.

No denominador temos

$$10! = 2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3} \cdot 7^{a_4}$$
$$11! = 2^{b_1} \cdot 3^{b_2} \cdot 5^{b_3} \cdot 7^{b_4} \cdot 11^{b_5}$$

A ordem de cada um dos expoentes é, usando o Teorema 8.20, para $10!$*:*

$$\begin{aligned}
\operatorname{ord}_2(10!) &= \left\lfloor \frac{10}{2} \right\rfloor + \left\lfloor \frac{10}{2^2} \right\rfloor + \left\lfloor \frac{10}{2^3} \right\rfloor = 5 + 2 + 1 = 8 \\
\operatorname{ord}_3(10!) &= \left\lfloor \frac{10}{3} \right\rfloor + \left\lfloor \frac{10}{3^2} \right\rfloor = 3 + 1 = 4 \\
\operatorname{ord}_5(10!) &= \left\lfloor \frac{10}{5} \right\rfloor = 2 \\
\operatorname{ord}_7(10!) &= \left\lfloor \frac{10}{7} \right\rfloor = 1.
\end{aligned}$$

Agora, para $11!$*:*

$$\begin{aligned}
\operatorname{ord}_2(11!) &= \left\lfloor \frac{11}{2} \right\rfloor + \left\lfloor \frac{10}{2^2} \right\rfloor + \left\lfloor \frac{10}{2^3} \right\rfloor = 5 + 2 + 1 = 8 \\
\operatorname{ord}_3(11!) &= \left\lfloor \frac{11}{3} \right\rfloor + \left\lfloor \frac{10}{3^2} \right\rfloor = 3 + 1 = 4 \\
\operatorname{ord}_5(11!) &= \left\lfloor \frac{11}{5} \right\rfloor = 2 \\
\operatorname{ord}_7(11!) &= \left\lfloor \frac{11}{7} \right\rfloor = 1 \\
\operatorname{ord}_{11}(11!) &= \left\lfloor \frac{11}{11} \right\rfloor = 1
\end{aligned}$$

Como temos $10!$ *elevado à décima potência, multiplicamos os expoentes de* $10!$ *por dez. Assim, temos*

$$\begin{aligned}
\operatorname{ord}_2(10!^{10}) &= 80 \\
\operatorname{ord}_3(10!^{10}) &= 40 \\
\operatorname{ord}_5(10!^{10}) &= 20 \\
\operatorname{ord}_7(10!^{10}) &= 10
\end{aligned}$$

Os expoentes no denominador $\mathrm{D} = (10!)^{10}11!$ *são*

$$\begin{aligned}
\operatorname{ord}_2(\mathrm{D}) &= 80 + 8 = 88\\
\operatorname{ord}_3(\mathrm{D}) &= 40 + 4 = 44\\
\operatorname{ord}_5(\mathrm{D}) &= 20 + 2 = 22\\
\operatorname{ord}_7(\mathrm{D}) &= 10 + 1 = 11\\
\operatorname{ord}_{11}(\mathrm{D}) &= 1
\end{aligned}$$

Verificamos se temos o necessário no numerador, $\mathrm{N} = 100!$*:*

$$\begin{aligned}
\operatorname{ord}_2(100!) &= \left\lfloor \frac{100}{2} \right\rfloor + \left\lfloor \frac{100}{2^2} \right\rfloor + \left\lfloor \frac{100}{2^3} \right\rfloor + \left\lfloor \frac{100}{2^4} \right\rfloor + \left\lfloor \frac{100}{2^5} \right\rfloor + \left\lfloor \frac{100}{2^6} \right\rfloor\\
&= 50 + 25 + 12 + 6 + 3 + 1\\
&= 97\\
&> 88.\\
\operatorname{ord}_3(100!) &= \left\lfloor \frac{100}{3} \right\rfloor + \left\lfloor \frac{100}{3^2} \right\rfloor + \left\lfloor \frac{100}{3^3} \right\rfloor + \left\lfloor \frac{100}{3^4} \right\rfloor\\
&= 33 + 11 + 3 + 1\\
&= 48\\
&> 44.\\
\operatorname{ord}_5(100!) &= \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{5^2} \right\rfloor\\
&= 20 + 4\\
&= 24\\
&> 22.\\
\operatorname{ord}_7(100!) &= \left\lfloor \frac{100}{7} \right\rfloor + \left\lfloor \frac{100}{7^2} \right\rfloor\\
&= 14 + 2\\
&= 16\\
&> 11.\\
\operatorname{ord}_{11}(100!) &= \left\lfloor \frac{100}{11} \right\rfloor\\
&= 9\\
&> 1.
\end{aligned}$$

E o número N/D *é inteiro*[17]*.* ◀

[17] $\mathrm{N}/\mathrm{D} = 590496880860450711582421357213329247657576820277824321023080623941171922612408075520 0.$

8.6 $\pi(n)$

A função $\pi(n)$ dá o número de primos menores ou iguais a n. Por exemplo,

$$\begin{array}{ll} \pi(2) = 1 & \pi(7) = 4 \\ \pi(3) = 2 & \pi(8) = 4 \\ \pi(4) = 2 & \pi(9) = 4 \\ \pi(5) = 3 & \pi(10) = 4 \\ \pi(6) = 3 & \pi(11) = 5 \end{array}$$

O Teorema 8.21 explicita uma relação entre $\pi(n)$ e $\phi(n)$,

Teorema 8.21. *Para quaisquer* k, n *inteiros positivos,*

$$\pi(n) \leq \left\lceil \frac{n}{k} \right\rceil \phi(k) + 2k$$

Demonstração. Se $k \geq n$, então o resultado segue trivialmente:

$$\pi(n) < n < s < 2k.$$

Suponha, portanto, que $n > k$ Sejam s o quociente e r o resto da divisão de n por k,

$$n = ks + r.$$

Visualizamos esta divisão como o agrupamento de s sequências de k números, seguidas de uma sequência de r números.

Na primeira sequência, $1, \ldots, k$, há no máximo k primos.

Agora, cada número m tal que $\mathrm{mdc}\,(m,k) > 1$ tem um fator primo p em comum com k, tal que $p < k$. Pelo menos um múltiplo de p estará dentre $k+1, \ldots, 2k$, portanto cada divisor de k que encontrarmos nos permite contar um múltiplo de primo no intervalo $k+1, \ldots, 2k$. Assim, haverá *no máximo* $\phi(k)$ primos em $k+1, \ldots 2k$. O mesmo vale para as outras sequências, $tk+1, \ldots (t+1)k$. Assim, contabilizamos (i) k primos na primeira sequência; (ii) $r < k$ primos na última sequência; e (iii) $(s-1)\phi(k)$ primos nas demais.

$$\begin{aligned} \pi(n) &\leq k + r + (s-1)\phi(k) \\ \pi(n) &\leq 2k + (s-1)\phi(k) \\ \pi(n) &\leq 2k + s\phi(k) \\ \pi(n) &\leq 2k + \left\lceil \frac{x}{k} \right\rceil \phi(k) \end{aligned}$$

□

8.7 Crescimento de $\pi(n)$

Nesta seção identificaremos limitantes superior e inferior para $\pi(n)$. O Teorema dos Números Primos, demonstrado em 1896 por Hadamard e Poussin, enuncia que

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1.$$

Não demonstraremos este Teorema. Ao invés disso, trabalharemos na demonstração (muito mais fácil) do Teorema de Chebychev. Chebychev– *Пафну́тий Льво́вич Чебышёв* em Russo –[18] A demonstração usualmente dada usa, além do Teorema de Polignac-Legendre (Teorema 8.20), somente conceitos elementares de Matemática. A demonstração do Teorema de Chebytchev incluída aqui depende de um Teorema conjecturado por Bertrand Bertrand[19] em 1845, e demonstrado por Chebychev em 1852.

Para cada inteiro n e primo p, definimos como r_p o expoente tal que $p^{r_p} \leq 2n$ e $p^{r_p+1} > 2n$.

O Lema 8.2 estabelece o fundamento para nossa demonstração do Teorema de Chebychev a respeito do crescimento de $\pi(n)$.

Lema 8.2. *Seja n inteiro positivo. Então*

$$\prod_{n<p<2n} p \;\Bigg|\; \binom{2n}{n} \;\Bigg|\; \prod_{p<2n} p^{r_p},$$

onde os números p no produtório são os primos entre n e $2n$.

Demonstração. Para o lado esquerdo, vemos que como

$$\binom{2n}{n} = \frac{(2n)!}{n!n!},$$

então p está na fatoração de $2n!$, porque é menor que $2n$, mas não está na fatoração de $n!n!$, porque é maior que n.

Já para o lado direito, $\binom{2n}{n} \mid \prod_{p<2n} p^{r_p}$,

$$\operatorname{ord}_p(2n!) = \sum_{i=1}^{r_p} \left\lfloor \frac{2n}{p^i} \right\rfloor$$

$$\operatorname{ord}_p(n!n!) = 2\operatorname{ord}_p(n!) = 2\sum_{j=1}^{r_p} \left\lfloor \frac{n}{p^j} \right\rfloor$$

[18] Pafnuty Lvovic Chebychev (1821-1894), Russo.

[19] Joseph Bertrand (1822-1900), Francês.

Tendo a ordem de p no numerador e no denominador, podemos calcular a ordem de p em $\binom{2n}{n}$.

$$\begin{aligned}\operatorname{ord}_p\binom{2n}{n} &= \sum_{i=1}^{r_p}\left(\left\lfloor\frac{2n}{p_i}-2\left\lfloor\frac{n}{p_i}\right\rfloor\right\rfloor\right)\\ &\leq \sum_{i=1}^{r_p} 1\\ &= r_p.\end{aligned}$$

Assim, como $\operatorname{ord}_p\binom{2n}{n} \leq r_p$, temos o resultado que queríamos:

$$\binom{2n}{n} \;\Big|\; \prod_{p<2n} p^{r_p}. \qquad \square$$

Com estes resultados já é possível demonstrar o Teorema de Chebychev.

Teorema 8.22 (de Chebychev)**.** *Existem constantes positivas A e B tais que, para todo $x > 2$,*

$$A\frac{x}{\log x} < \pi(x) < B\frac{x}{\log x}.$$

Demonstração. A demonstração de divisibilidade no Lema 8.2 tem o único propósito de nos ajudar a demonstrar uma desigualdade, já que para $a, b \in \mathbb{Z}$, $a \mid b \Rightarrow a \leq b$. Pelo Lema,

$$\prod_{n<p<2n} p \;\leq\; \binom{2n}{n} \;\leq\; \prod_{p<2n} p^{r_p}.$$

Agora, compare número $n^{\pi(2n)-\pi(n)}$ com $\prod_{n<p<2n} p$

$$\begin{aligned}n^{\pi(2n)-\pi(n)} &= n\cdot n\cdot n\cdots n\\ \prod_{n<p<2n} p &= p_1\cdot p_2\cdots p_k\end{aligned}$$

Há $\pi(2n)-\pi(n)$ fatores em ambos os casos, mas cada um dos p_i é maior que n, logo

$$n^{\pi(2n)-\pi(n)} \leq \prod_{n<p<2n} p$$

Da mesma forma, comparamos $(2n)^{\pi(2n)}$ com $\prod_{p<2n} p^{r_p}$.

$$\begin{aligned}(2n)^{\pi(2n)} &= (2n)\cdot(2n)\cdots(2n)\\ \prod_{p<2n} p^{r_p} &= p_1^{r_1 p}\cdot p_2^{r_2 p}\cdots p_k^{r_k p}\end{aligned}$$

Há $\pi(2n)$ fatores nas duas expressões, e cada $p_i^{r_{p_i}}$ é menor que $2n$, portanto

$$\prod_{p<2n} p^{r_p} \leq (2n)^{\pi(2n)}.$$

Disso concluimos que

$$n^{\pi(2n)-\pi(n)} \leq \prod_{n<p<2n} p \leq \binom{2n}{n} \leq \prod_{p<2n} p^{r_p} \leq (2n)^{\pi(2n)}$$

Tomando o logaritmo da desigualdade,

$$[\pi(2n) - \pi(n)] \log(n) \leq \log \binom{2n}{n} \leq \pi(2n) \log(2n) \tag{8.7}$$

Observamos que

$$\binom{2n}{n} \geq 2^n$$

$$\log \binom{2n}{n} \geq n \log(2) \tag{log}$$

Do lado direito da desigualdade 8.7, obtemos o limitante inferior para $\pi(n)$:

$$\pi(2n) \log(n) \geq \log \binom{2n}{n}$$

$$\pi(2n) \log(n) \geq n \log(2)$$

$$\pi(2n) \geq \log(2) \left(\frac{n}{\log n} \right)$$

A desigualdade que obtivemos é para $2n$, e não para n; no entanto,

$$\begin{aligned} \pi(m) &\geq \pi\left(2 \left\lfloor \frac{m}{2} \right\rfloor\right) \\ &\geq C \frac{\left\lfloor \frac{m}{2} \right\rfloor}{\log\left(\left\lfloor \frac{m}{2} \right\rfloor\right)} && \text{(para algum } C > 0\text{)} \\ &\geq B \frac{m}{\log m}, && \text{(para algum } B > 0\text{)} \end{aligned}$$

e demonstramos que $\pi(n) \geq B\ n/\log(n)$.

Passamos ao limitamte superior. Destacamos inicialmente que

$$\binom{2n}{n} \leq 2^{2n}$$
$$\log \binom{2n}{n} \leq 2n \log(2). \tag{log}$$

Escrevemos novamente o lado esquerdo da desigualdade 8.7.

$$\begin{aligned}
\left[\pi(2n) - \pi(n)\right] \log(n) &\leq \log \binom{2n}{n} \\
\left[\pi(2n) - \pi(n)\right] \log(n) &\leq 2n \log(2) \\
\pi(2n) - \pi(n) &\leq 2 \log(2) \frac{n}{\log(n)}
\end{aligned}$$

É simples verificar, por indução, e usando os resultado já obtido até agora, que

$$\pi(2^k) \leq 3\frac{2^k}{k}. \tag{8.8}$$

Como $n/\log(n)$ é monotonicamente crescente para $n \geq e$, suponha que $2^k < n \leq 2^{k+1}$ para algum k. Então

$$\begin{aligned}
\pi(n) &\leq \pi(2^{k+1}) && (n \leq 2^{2^k+1}) \\
&\leq 6\frac{2^k}{k+1} && \text{(por (8.8))} \\
&= 6\frac{\log(2)2^k}{\log(2)(k+1)} \\
&= 6\log(2)\frac{2^k}{\log(2)k + \log(2)} \\
&= B\frac{2^k}{\log(2)k}\log(2)k + \log(2) && (B = 6\log 2) \\
&< B\frac{2^k}{\log(2)k} \\
&= B\frac{2^k}{\log(2^k)} \\
&\leq B\frac{n}{\log n}. && (2^k < n)
\end{aligned}$$

Mostramos, portanto, que $\pi(n) < B\frac{n}{\log(n)}$, e a demonstração termina aqui. □

Exercícios

Ex. 207 — Determine $\sigma(p^n)$ e $d(p^n)$, onde p é primo e $n \in \mathbb{N}$.

Ex. 208 — Determine forma fechada para $\sigma(n)$ e $d(n)$, a partir da fatoração de n.

Ex. 209 — Mostre que, se n é composto, $\sigma(n) > n + \sqrt{n}$.

Ex. 210 — Encontre todos os inteiros positivos n tais que $\sigma(n) = n + 8$.

Ex. 211 — Mostre que se $\sigma(n)$ é ímpar, então n é quadrado ou dobro de quadrado.

Ex. 212 — Mostre que se p é primo, $\phi(p^n) = p^n - p^{n-1}$.

Ex. 213 — Mostre que se $n > 2$ então $\phi(n)$ é par.

Ex. 214 — Mostre que para todos $n, k \in \mathbb{N}$,

$$\phi(n^k) = n^{k-1}\phi(n).$$

Ex. 215 — Resolva:

a) $\phi(n) = 12$

b) $\phi(n) = n/2$

c) $\phi(\phi(n)) = 2^{20}3^8$

Ex. 216 — Mostre os detalhes da demonstração do Teorema 8.2.

Ex. 217 — Prove que $\phi(2k)$ é $2\phi(k)$ se k é par, ou $\phi(k)$ se k é ímpar.

Ex. 218 — Prove que para todo n inteiro positivo,

$$\sum_{i=1}^{n} M\left(\left\lfloor \frac{n}{i} \right\rfloor\right) = 1.$$

Ex. 219 — Prove que para todo n inteiro positivo,

$$n = \phi(n) \sum_{d|n} \frac{\mu^2(d)}{\phi(d)}.$$

Ex. 220 — Sejam $f : \mathbb{N} \to \mathbb{R}$ e $g : \mathbb{N} \to \mathbb{R}$, com

$$g(n) = \sum_{d|n} f(d).$$

Prove que

$$f(n) = \sum_{\substack{d|n \\ n \text{ livre de quadrados}}} (-1)^{p(n/d)} g(d),$$

onde $p(n/s)$ é a quantidade de primos distintos na fatoração de n/d

Ex. 221 — Demonstre o Teorema 8.3.

Ex. 222 — Prove que se $f(n)$ é uma função aritmética multiplicativa, então

$$f(\text{mdc}\,(a,b)) \cdot f(\text{mmc}(a,b)) = f(a)f(b).$$

Ex. 223 — Prove que $\phi(m)\phi(n) = \phi(\text{mdc}\,(m,n))\phi(\text{mmc}(m,n))$.

Ex. 224 — Seja n um inteiro positivo. O *radical* de um n é o produto dos primos *distintos* na fatoração (ou seja, é a fatoração de n, mas modificada para que todo primo tenha expoente um). Denotamos o radical de n por $\text{rad}(n)$. Por exemplo, $600 = (2^3)(3)(5^2)$, então $\text{rad}(600) = (2)(3)(5) = 30$. Prove que

$$\frac{\phi(n)}{n} = \frac{\phi(\text{rad}(n))}{\text{rad}(n)}.$$

Ex. 225 — Prove que para todo inteiro positivo n,

$$\sigma(n) = \prod_{d|n} \left(\frac{p^{a+1} - 1}{p - 1} \right).$$

Ex. 226 — Prove que

$$\mu(n) = \sum_{\substack{1 \le k \le n \\ \text{mdc}(k,n)=1}} e^{2\pi i k/n}$$

Ex. 227 — Calcule

$$\int_0^\infty \lfloor x \rfloor \, e^{-x} dx$$
$$\int_0^{k\pi} \lfloor x \rfloor \operatorname{sen}(x) dx$$

Ex. 228 — Prove que p é primo se e somente se

$$\sum_{j-1}^{\infty} \left(\left\lfloor \frac{n}{j} \right\rfloor - \left\lfloor \frac{n-1}{j} \right\rfloor \right) = 2.$$

Ex. 229 — Modifique o argumento da demonstraçõa de Erdös para a infinitude dos primos (Teorema 5.8 – enunciado na página 103, prova na página 104), para obter uma cota inferior para $\pi(n)$.

Ex. 230 — Prove que para $x \in \mathbb{R}$ não inteiro,

$$\lfloor x \rfloor = x - \frac{1}{2} + \frac{1}{\pi} \sum_{j=1}^{\infty} \frac{\operatorname{sen}(2\pi x j)}{j}$$

Ex. 231 — Seja $f : [1, 45] \to \mathbb{Z}$ (o domínio de f é o intervalo $[1, 45]$),

$$f(x) = \left\lfloor \frac{x}{7} \right\rfloor \left\lfloor \frac{37}{x} \right\rfloor.$$

Qual é a cardinalidade da imagem de $f(x)$?

Ex. 232 — Encontre n tal que $\phi(\sigma(2^n)) = 2^n$.

Ex. 233 — Encontre expressões fechadas para

a) $\sum_{d|n} \mu(d)\sigma(d)$

b) $\sum_{d|n} \frac{\mu(d)}{d}$

c) $\sum_{d|n} \mu(d)\phi(d)$

d) $\sum_{d|n} \mu^2(d)\phi^2(d)$

e) $\sum_{d|n} \frac{\mu(d)}{\phi(d)}$

Ex. 234 — Resolva:

a) $\phi(3^a 5^b) = 360$

b) $\phi(n) = 16$

Ex. 235 — Prove que

$$\prod_{p|n}\left(1-\frac{1}{p}\right)=\sum_{d|n}\frac{\mu(d)}{d}.$$

Ex. 236 — Prove que a definição dada a seguir é equivalente à Definição 8.8.

Definição 8.12. *A **função** μ **de Moebius** é a <u>única</u> função aritmética tal que*

$$\begin{aligned}\mu(1)&=1\\ \sum_{d|n}\mu(d)&=0,\quad \forall n\in\mathbb{N},\ n>1.\end{aligned}$$

◀

Ex. 237 — Determine a quantidade de funções $f:\mathbb{Z}_n\to n$ multiplicativas e crescentes, com $f(2)=4$. Determine também para quantos valores estas funções são iguais (para quantos n vale $f_i(k)=f_j(k)$).

Ex. 238 — Prove que a soma dos números k menores que n, tais que $\operatorname{mdc}(k,n)=1$, é

$$\frac{n\phi(n)}{2}.$$

Ex. 239 — Demonstre o Teorema 8.14.

Ex. 240 — Demonstre[20] o Teorema 8.15.

Ex. 241 — Prove que se $n=n_1+n_2+\cdots+n_k$ então

$$\frac{n!}{n1!\cdot n2!\cdots n_k!}\quad\in\mathbb{Z}.$$

Ex. 242 — Prove que a seguinte fórmula (similar à inversão de Moebius) vale.

[20] Este Teorema foi demonstrado por Gauss no *Disquisitiones* (no artigo 81).

Gauss, Johann Carl Friedrich. **Disquisitiones Arithmeticae**. [*S. l.*], 1801.

Gauss não usou a fórmula de inversão de Möbius, mas é possível usá-la. Na verdade, Gauss não usa a função de Möbius em nenhuma outra passagem do *Disquisitiones*, que foi publicado inicialmente em 1801 (trinta e um anos antes de Möbius publicar o tratamento sistematizado da fórmula de inversão em 1832).

Sejam duas funções f e g. Então,

$$g(x) = \sum_{j=1}^{\lfloor x \rfloor} f\left(\frac{x}{j}\right)$$

se e somente se

$$f(x) = \sum_{j=1}^{\lfloor x \rfloor} \mu(j) g\left(\frac{x}{j}\right).$$

Ex. 243 — Com quantos zeros termina $100!/40!$?

Ex. 244 — Qual é a maior potência de 40 que divide $40!$?

Ex. 245 — Na demonstração do Teorema de Chebychev (Teorema 8.22), mencionamos que é possível provar, por indução, que

$$\pi(2^k) \leq 3\frac{2^k}{k}.$$

Mostre os detalhes.

Ex. 246 — Prove que

$$\pi(n) = \sum_{j=2}^{n} \left\lfloor \frac{(j-1)! + 1}{j} - \left\lfloor \frac{(j-1)!}{j} \right\rfloor \right\rfloor$$

Ex. 247 — Prove que (* Legendre) se a fatoração de n é $p_1 p_2 \dots p_n$, então

$$\pi(n) = \pi\left(\sqrt{n}\right) - 1 + \lfloor n \rfloor - \sum_i \left\lfloor \frac{n}{p_i} \right\rfloor + \sum_{i<j} \left\lfloor \frac{n}{p_i p_j} \right\rfloor - \sum_{i<j<k} \left\lfloor \frac{n}{p_i p_j p_k} \right\rfloor + \cdots$$

Ex. 248 — Definmos a *função de Merten* e *matriz de Redheffer*
Definição 8.13 (função de Merten)**.** *A* ***função de Merten****,* $M(n)$ *dá a soma de* $\mu(k)$ *para todo* $k \leq n$*:*

$$M(n) = \sum_{1 \leq k \leq n} \mu(k). \qquad \blacktriangleleft$$

Por exemplo,

$$\begin{aligned} M(4) &= \mu(1) + \mu(2) + \mu(3) + \mu(4) \\ &= 1 + (-1) + (-1) + 0 = -1. \end{aligned}$$

Merten conjecturou que $|M(x)|$ seria sempre estritamente menor do que x, mas a conjectura foi provada falsa por Odlyzko e Riele em 1985.

Definição 8.14 (matriz de Redheffer)**.** *A* ***matriz de Redheffer de ordem*** n*, denotada* $R_{n\times n}$ *é uma matriz quadrada de ordem* n*, com elementos* $r_{ij} = 1$ *se* $j = 1$ *ou* $i \mid j$*; caso contrário,* $r_{ij} = 0$. ◀

Por exemplo,

$$R_{6\times 6} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Prove que para todo inteiro positivo n,

$$M(n) = \det R_{n\times n}.$$

Ex. 249 — Seja p primo. A função $f(n) = \operatorname{mdc}(p, n)$ é multiplicativa? E se o inteiro p não for primo?

Ex. 250 — A função de Merten é multiplicativa?

Ex. 251 — Prove o Teorema 8.9.

Capítulo 9

Resíduos Quadráticos

Limitamo-nos até o momento ao estudo de congruências lineares – mais especificamente, as da forma $ax \equiv b \pmod{m}$. Este Capítulo trata de congruências envolvendo quadrados.

O problema de resolver equações quadráticas na forma geral pode ser reduzido ao de resolver equações da forma $x^2 = a \pmod{p}$, de que tratamos a partir de agora. Ao final deo Capítulo mostramos como resolver a equação geral de segundo grau tendo método apenas para a equação mais simples $x^2 \equiv a \pmod{p}$.

9.1 Resíduos Quadráticos

Inicialmente, damos um nome aos quadrados módulo m.

Definição 9.1 (resíduo quadrático)**.** *Dizemos que a é um **resíduo quadrático** módulo m se a equação $x^2 \equiv a \pmod{m}$ tem solução.*

Denotamos por Q_n o conjunto (ou ainda, o grupo) dos resíduos quadráticos módulo n. ◀

O critério de Euler permite determinar quando um elemento é quadrado módulo p, se p for primo.

Teorema 9.1 (critério de Euler)**.** *Se p é primo, então a é resíduo quadrático módulo p se e somente se*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Demonstração. Se a é resíduo quadrático módulo p, então

$$\begin{aligned} a^{\frac{p-1}{2}} &\equiv (x^2)^{\frac{p-1}{2}} && \pmod{p} \\ &\equiv x^{p-1} && \pmod{p} \\ &\equiv 1 && \pmod{p}. \qquad \text{(pelo Teorema de Euler)} \end{aligned}$$

Agora suponha que $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Como p é primo, deve haver alguma raiz primitiva g módulo p, e existe algum k tal que $g^k \equiv a \pmod{p}$. Agora reescrevemos a congruência do enunciado,

$$(g^k)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Mas a ordem de g é $p-1$, porque é raiz primitiva, e portanto $k(p-1)/2$ deve ser múltiplo de $p-1$. Então $k/2$ é inteiro, e k é par. Como $g^k \equiv g^{2j} \equiv a \pmod{p}$, a é resíduo quadrático. □

Um exemplo com módulo 13: elevamos 7 ao quadrado; 49 é resíduo quadrático módulo 13; mas como $49 \equiv 10 \pmod{13}$, então 10 é resíduo quadrático módulo 13. Observamos que que $10^6 \equiv 1 \pmod{13}$, porque $10^3 10^3 = 130^6$ e $10^6 = 76923(13) + 1$. Usamos o Teorema de Euler e confirmamos que 10 é resíduo quadrático módulo 13:

$$10^{12} \equiv 1 \pmod{13}.$$

Corolário 9.1. *A quantidade de resíduos quadráticos módulo* p *é exatamente igual à de resíduos não quadráticos.*

Demonstração. Seja g um gerador de $\mathbb{Z}_p$. Podemos descrever $\mathbb{Z}_p$, portanto como

$$\mathbb{Z}_p = \left\{ g^0, g^1, g^2, \ldots, g^{\frac{p-1}{2}-1}, g^{\frac{p-1}{2}}, g^{\frac{p-1}{2}+1}, \ldots, g^{p-2} \right\}.$$

Temos $p-1$ elementos em $\mathbb{Z}_p$ listados acima (de g^0 a g^{p-2}, porque $g^{p-1} \equiv 1 \equiv g^0 \pmod{p}$).
Então os quadrados módulo $\mathbb{Z}_p$ são

$$\begin{aligned} \mathbb{Z}_p &= \left\{ g^0, g^2, g^4, \ldots, g^{p-1-2}, g^{p-1}, g^{p-1+2}, g^{p-1+4}, \ldots, g^{2p-4} \right\}. \\ &= \left\{ g^0, g^2, g^4, \ldots, g^{p-3}, g^0, g^{p-1+2}, g^{p-1+4} \ldots, g^{2p-4} \right\}. \quad (g^{p-1} \equiv 1 \equiv g^0) \\ &= \left\{ g^0, g^2, g^4, \ldots, g^{p-3}, g^0, g^{p-1}g^2, g^{p-1}g^4 \ldots, g^{p-1}g^{p-3} \right\}. \\ &\qquad\qquad \text{(fatore } p-1 \text{ no expoente)} \\ &= \left\{ g^0, g^2, g^4, \ldots, g^{p-3}, g^0, g^2, g^4 \ldots, g^{p-3} \right\}. \end{aligned}$$

Notamos que a sequência se repete duas vezes. Temos somente que mostrar que estes são todos incongruentes modulo p Suponha que r^2 e s^2 sejam congruentes módulo p. Mas se $r^2 \equiv s^2 \pmod{p}$, então e $r^2 - s^2 \equiv 0 \pmod{p}$,

ou seja, $(r+s)(r-s) \equiv 0 \pmod{p}$, e $r \equiv \pm s \pmod{p}$. □

Por exemplo, para $p = 11$ há cinco resíduos quadráticos $(1, 3, 4, 5, 9)$, e cinco não quadráticos $(2, 6, 7, 8, 10)$.
O Exercício 267 pede a demonstração do Teorema 9.2.

Teorema 9.2. *O conjunto Q_n dos resíduos quadráticos módulo n é subgrupo de U_n.*

Há duas funções que facilitam cálculos a respeito de resíduos quadráticos – estas são chamadas de *"símbolo de Legendre"* e *"símbolo de Jacobi"*.

Definição 9.2 (símbolos de Legendre e Jacobi)**.** *Se p é primo ímpar, então o **símbolo de Legendre** para a e p é*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{se } a \not\equiv 0 \pmod{p} \text{ e } a \text{ é resíduo quadrático módulo } p \\ 0 & \text{se } p \mid a \\ -1 & \text{em outros casos.} \end{cases}$$

*Se m não é primo, e $m = p_1 p_2 \cdots p_k$, definimos o **símbolo de Jacobi***

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right)$$

Os símbolos de Legendre e Jacobi podem também ser denotados por (a/p), (a/m). ◀

Como já mencionamos que as classes de congruência de resíduos quadráticos módulo 11 são $1, 3, 4, 5, 9$, então

$$\left(\frac{5}{11}\right) = +1, \quad \left(\frac{6}{11}\right) = -1, \quad \left(\frac{22}{11}\right) = 0,$$

O critério de Euler pode ser reescrito, portanto como "$(a/p) = +1$ se e somente se $a^{(p-1)/2} \equiv 1 \pmod{p}$".

Teorema 9.3. *Se p é primo e $a \equiv b \pmod{p}$, então*

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \tag{i}$$

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right) \tag{ii}$$

Demonstração. (i) segue naturalmente da definição do símbolo de Legendre:

- se $(a/p) = 0$, então $p \mid a$; mas se $a \equiv b \pmod{p}$, então $p \mid b$, e $(b/p) = 0$;

- se $(a/p) = 1$, então a é quadrado módulo p; mas se $b \equiv a \pmod{p}$, então $b \equiv a \equiv x^2 \pmod{p}$, e $(b/p) = 1$;

- se $(a/p) = -1$, então a não se enquadra nos casos já discutidos, e se $b \equiv a \pmod{p}$, b também não pode se enquadrar neles. Assim, $(b/p) = -1$.

(ii) é verdadeira porque

- se $(a/p) = 0$, então $p \mid a$, e $p \mid ab$, logo $(ab/p) = 0$;

- se $(a/p) = +1$, então $a \equiv b \equiv x^2 \pmod{p}$, e $ab \equiv x^2x^2 \pmod{p}$, logo $(ab/p) = 1$;

- se $(a/p) = -1$, então como $a \equiv b \pmod{p}$, temos $ab \equiv aa \pmod{p}$, e $(ab/p) = 1$. □

Teorema 9.4. *Se p é primo, então*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Demonstração. Se $p \mid a$, então $p \mid a^{\frac{p-1}{2}}$, e $a^{\frac{p-1}{2}} \equiv 0 \pmod{p}$, logo

$$\left(\frac{a}{p}\right) = 0 \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Pelo critério de Euler, se a é resíduo quadrático módulo p, então

$$\left(\frac{a}{p}\right) = 1 \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Se $a \not\equiv 0 \pmod{p}$ não é resíduo quadrático, então

$$\begin{aligned} a^{\frac{p-1}{2}} &= (g^{2k+1})^{\frac{p-1}{2}} && \pmod{p} \\ &\equiv g^{\frac{(2k+1)(p-1)}{2}} && \pmod{p} \\ &\equiv g^{k(p-1)} g^{\frac{p-1}{2}} && \pmod{p} \\ &\equiv (1)(-1) && \pmod{p} \\ &\equiv -1 && \pmod{p} \end{aligned}$$

Assim, nos três casos (quando $(a/p) = -1, 0 + 1$), o enunciado vale. □

Terminamos com dois Lemas e um Corolário, cujas demonstrações são pedidas nos Exercícios 260, 261 e 262.

Lema 9.1. *Se* p *é primo ímpar,*

$$\left(\frac{-1}{p}\right) = \begin{cases} +1 & \text{se } p = 4k+1, \\ -1 & \text{se } p = 4k+3. \end{cases}$$

Lema 9.2. *Se* p *é um primo ímpar, então*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Corolário 9.2. *Se* $n \in \mathbb{Z}$ *é ímpar, então*

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}.$$

9.2 Reciprocidade Quadrática

A Lei da Reciprocidade Quadrática[1], que enunciamos a seguir, foi chamada por Gauss de "Teorema de Ouro"[2]. Observada e estudada por Euler e Legendre (a partir de observações de Fermat), foi demonstrada somente mais tarde por Gauss. que apresentou nada menos que seis demonstrações desse Teorema; depois dele, surgiram mais de trezentas outras[3] (incluindo pequenas variações, mas ainda assim um número notável). O próprio Gauss declarou ter insistido em novas demonstrações por estar procurando uma que se prestasse a generalizações [4].

A Lei da Reciprocidade Quadrática teve um papel fundamental no desenvolvimento da teoria algébrica de números e teoria dos corpos de classes; e os inteiros Gaussianos são parte de uma tentativa de Gauss de estudar maneiras de generalizar este Teorema.

---

[1] **Gauss**, Johann Carl Friedrich. **Disquisitiones Arithmeticae**. [*S. l.*], 1801.

Seção IV, art. 131. O texto não tem capítulos, apenas "seções", e no estilo usado por Gauss (Gauß), o texto é uma sequência de "artigos", cada um compreendendo alguns parágrafos. O próprio Gauss discute, no artigo 151, a história do Teorema.

[2] Não quando o enunciou no *Disquisitiones*, mas informalmente em correspondências.

[3] Dois livros sobre demonstrações da reciprocidade quadrática:

Baumgart, Oswald. **The Quadratic Reciprocity Law: a collection of classical proofs**. [*S. l.*]: Birkhauser, 2015.

Lemmermeyer, Franz. **Reciprocity Laws: from Euler to Eisenstein**. [*S. l.*]: Springer, 2000.

[4] **Goldman**, Jay R. **The Queen of Mathematics: A Historically Motivated Guide to Number Theory**. Natick, MA: A. K. Peters, 1998.

Pag. 216.

Teorema 9.5 (Lei da Reciprocidade Quadrática, como enunciado por Gauss)**.** *Se* p *for um número primo da forma* $4n+1$*,* $+p$ *será um resíduo ou não resíduo de qualquer número primo que, tomado positivamente, é um resíduo ou não resíduo de* p*. Se* p *for da forma* $4n+3$*,* $-p$ *terá a mesma propriedade*[5]*.*

No parágrafo seguinte, Gauss justifica ter nomeado este fato como "Teorema Fundamental":

> Como quase tudo o que pode ser dito sobre os resíduos quadráticos se baseia neste teorema, a denominação de *teorema fundamental*, que utilizaremos a seguir, não estará fora de lugar[6].

Enunciamos, agora de maneira contemporânea, a Lei da Reciprocidade Quadrática[7].

Teorema 9.6 (Lei da Reciprocidade Quadrática)**.** *Sejam* $p \neq q$ *dois primos ímpares, e considere as equações*

$$x^2 \equiv q \pmod{p}$$
$$x^2 \equiv p \pmod{q}$$

Se os dois primos forem da forma $4k+3$*, então uma delas tem solução e a outra não.*
Se pelo menos um dos primos for da forma $4k+1$*, então ou as duas equações tem solução, ou nenhuma tem.*

Reformularemos agora o enunciado, de maneira a facilitar a demonstração[8]

[5] Gauss (Gauß) escreveu o *Disquisitiones Arithmeticae* em Latim, e o enunciado original é *Si p est numerus primus formae* $4n+1$*, erit* $+p$*, si vero* p *formae* $4n+3$*, erit* $-p$ *residuum vel non residuum cuinsuis numeri primi qui positive acceptus ipsius* p *est residuum vel non-residuum.*

[6] *Quia omnia fere quae de residuis quadraticis dici possunt, huic theoremati innituntur, denominatio theorematis fundamentalis, qua in sequentibus vtemur, haud absona erit.*

[7] Foi Adrian-Marie Legendre quem a enunciou na forma que conhecemos. Legendre deu uma demonstraçõa incompleta do Teorema em 1788. Um artigo sobre os estudos feitos por Legendre:

Weintraub, Steven H. On Legendre's Work on the Law of Quadratic Reciprocity. **The American Mathematical Monthly**, v. 118, n. 3, p. 210–216, 2011.

[8] Poderíamos também dizer:

- Se p e q forem da forma $4k+3$:
  - $p \in Q_q$ **e** $q \notin Q_p$, **ou**
  - $p \notin Q_q$ **e** $q \in Q_p$.
- Se pelo menos um dos primos for da forma $4k+1$:
  - $p \in Q_q$ **e** $q \in Q_p$, **ou**
  - $p \notin Q_q$ **e** $q \notin Q_p$.

Mas isto não facilita a demonstração.

– usaremos o símbolo de Legendre, que formulou o mesmo teorema usando seu símbolo[9].

Teorema 9.7 (Lei da Reciprocidade Quadrática)**.** *Sejam* $p \neq q$ *dois primos ímpares. Então*

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right),$$

exceto quando p *e* q *são da forma* $4k+3$*, quando vale a negação da igualdade acima.*

Considere a expressão

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

analisando as possibilidades para os expoentes:

p, q	$\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$		paridade	valor
$4k+1, 4j+1$	$\frac{(4k)(4j)}{4}$	$= 4kj$	par	$+1$
$4k+3, 4j+3$	$\frac{(4k+2)(4j+2)}{4}$	$= 4kj + 2j + 2k + 1$	ímpar	-1
$4k+3, 4j+1$	$\frac{(4k+2)(4j)}{4}$	$= 16kj + 8j$	par	$+1$

Isto nos permite reformular a Lei da Reciprocidade quadrática sem mencionar explicitamente os tipos de primo ($4k+1$, $4k+3$).

Teorema 9.8 (Lei da Reciprocidade Quadrática)**.** *Se* $p \neq q$ *são primos ímpares, então*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Isso nos dá um método para determinar se um número é resíduo quadrático módulo um primo p.

Exemplo 9.1. *Tomamos dois primos ímpares,* 11 *e* 313*, e verificaremos se* 11 *é resíduo quadrático módulo* 313*. A lei da reciprocidade quadrática será usada nesse processo.*
Como $313 = 4k + 1$*, pela lei da reciprocidade quadrática,*

$$\left(\frac{11}{313}\right) = \left(\frac{313}{11}\right).$$

[9]Para quaisquer números primos (distintos e ímpares) m e n, se eles não forem ambos da forma $4x + 3$, sempre valerá $(m/n) = (n/m)$, e se forem ambos da forma $4x + 3$, valerá $(m/n) = -(n/m)$. Estes dois casos gerais são combinados na fórmula

$$\left(\frac{n}{m}\right) = (-1)^{\left(\frac{m-1}{2}\right)\left(\frac{n-1}{2}\right)}\left(\frac{m}{n}\right).$$

A apresentação contemporânea é ligeiramente diferente, como se poderá verificar no enunciado neste texto.

Como $(313/11)$ *deermina "se* 313 *é quadrado módulo* 11*" podemos sSimplificar, já que* $313 \equiv 5 \pmod{11}$*:*

$$\left(\frac{11}{313}\right) = \left(\frac{5}{11}\right)$$

Mas como $5 = 4k + 1$*, pela reciprocidade quadrática* $(5/11) = (11/5)$*:*

$$\left(\frac{11}{313}\right) = \left(\frac{11}{5}\right)$$

Mas $11 \equiv +1 \pmod{5}$*, e* 1 *sempre é resíduo quadrático, portanto* $(11/5) = +1$*.*

$$\left(\frac{11}{313}\right) = +1,$$

o que significa que 11 *é quadrado módulo* 313*. E realmente,* $18^2 \equiv 11 \pmod{313}$*.* ◀

Apresentamos quatro das demonstrações mais simples deste Teorema: a primeira é de Gauss, por indução (é a primeira demonstração conhecida deste Teorema); a de Rousseau, que depende apenas de resultados básicos da Teoria de Números; a de Eisenstein, através da contagem de pontos em um reticulado; e finalmente uma outra demonstração, de Gauss, usando raízes da unidade.

As seis demonstrações de Gauss são listadas a seguir. Antes destas, há uma de Legendre, mas incompleta. Depois das demonstrações de Gauss surgiram mais de trezentas. A tabela é baseada em uma compilação de Franz Lemmermeyer.

ano	método	onde
1801	indução	*Disquisitiones Arithmeticae*
1801	formas quadráticas	*Disquisitiones Arithmeticae*
1808	Lema de Gauss	*Theorematis arithmetici demonstratio nova*
1811	raízes da unidade (ciclotomia)	*Summatio serierum quarundam singularium*
1818	Lema da Gauss	*Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et amplicationes novae*
1818	somas de Gauss	*Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et amplicationes novae*

Essas demonstrações começaram com um argumento indutivo e combinatório, que parecia desconectado da estrutura algébrica que evidentemente existia, cada vez mais valorizando aspectos algébricos e possibilidade de abstração. As mais de trezentas demonstrações deste teorema tem um motivo: é certo que o teorema vale, mas existe, por parte dos matemáticos, uma dificuldade em compreender *porquê* ele vale. D'Alessandro pondera[10] que as demonstrações costumam ser transparentes, mas rasas ou profundas, mas pouco transparentes, e menciona que Fernando Gouvêa, por exemplo, comenta[11] a demonstração de Eisenstein (que é apresentada neste texto):

> *A prova funciona, mas é notável que não nos dá absolutamente nenhum insight sobre porque o teorema é verdadeiro. Em particular, não dá nenhuma conexão entre a "vida módulo* p *" e a "vida módulo* q *". Toda vez que apresento esta demonstração a estudantes, chamo atenção ao sentimento de que sim, tudo se encaixa corretamente, mas está coreto porque o teorema é verdadeiro.*

[10] **D' Alessandro**, William. Proving quadratic reciprocity: explanation, disagreement, transparency and depth. **Synthese**, v. 198, p. 8621–8664, 2021.

[11] Gouvêa faz a afirmação em um *review*:

Gouvêa, Fernando. Review of The quadratic reciprocity law: A collection of classical proofs, by Oswald Baumgart (F. Lemmermeyer, Ed. and Trans.) **MAA Reviews**, 2015.

É difícil dizer que (e eu não acredito) que contar pontos em um retângulo explique porquê o teorema é verdadeiro.

9.2.1 Demonstração de Gauss (a primeira, por indução) – rascunho

A primeira demonstração que Gauss deu para a Lei da Reciprocidade Quadrática é por indução. Ela não é muito transparente (é uma sequência obscura de manipulações), não permite facilmente generalizações, e não tem profundidade (não permite perceber ligações entre o enunciado do Teorema com outros conceitos/áreas). Um rascunho desta demonstração é incluído aqui para comparação com as outras[12]

Lema 9.3. *Seja* q *um primo da forma* $4k+1$*. Então existe um primo ímpar* p *tal que*

$$\left(\frac{q}{p}\right) = -1.$$

Demonstração. (da Lei da Reciprocidade Quadrática) Seja

$$p^* = (-1)^{\frac{p-1}{2}} p.$$

A idéia é que p^* seja igual a p, mas com sinal $+1$ se p é da forma $4k+1$ ou sinal -1 se p é da forma $4k+3$.
Suponha $p < q$. A demonstração é por indução em q. A base é

$$\left(\frac{3^*}{5}\right) = \left(\frac{-3}{5}\right) = \left(\frac{2}{5}\right) = -1 = \left(\frac{5}{3}\right).$$

Agora suponha $q > 5$, e suponha que $(s^*/r) = (r/s)$ para todos os pares de primos distintos r, s menores que q. O passo é feito em três casos:

i) $(p^*/q) = +1$. Prove que $(q/p) = +1$.

ii) $(p^*/q) = -1, q = 4k+3$. Prove que $(q/p) = -1$.

iii) $(p^*/q) = -1, q = 4k+1$. Prove que $(q/p) = -1$.

A partir de (i), (ii) e (iii), conclua a validade da Lei da Reciprocidade Quadrática. □

Esta demonstração não mostra claramente nenhuma relação com outras áreas da Matemática; não é generalizável; e os argumentos não são muito intuitivos. Gauss continuou trabalhando no teorema, até encontrar essas qualidades em outras demonstrações.

[12] Uma exposição completa da demonstração é dada por Daniel Flath no livro

Flath, Daniel. **Introduction to Number Theory**. [*S. l.*]: John Wiley e Sons, 1989.

9.2.2 Demonstração de Rousseau

A demonstração a seguir, originalmente dada por G. Rousseau[13][14] em 1991, é elementar: usa apenas o Teorema de Wilson, o critério de Euler e o Teorema Chinês dos Restos (o próprio Rousseau aponta que a demonstração deixa claro que a lei de reciprocidade "é uma consequência simples do teorema chinês dos restos". Também é bastante transparente.

Demonstração. (da Lei da Reciprocidade Quadrática) Sejam $p \neq q$ dois primos ímpares. Sejam

$$\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$$
$$\mathbb{Z}_q^* = \{1, 2, \ldots, q-1\}$$

os grupos de unidades módulo p e q (que são diferentes de $\mathbb{Z}_p$ e $\mathbb{Z}_q$ por excluírem o zero). Seja também

$$\mathbb{Z}_{pq}^* = \left\{1 \leq x \leq pq-1 \;\middle|\; \operatorname{mdc}(x, pq) = 1\right\}.$$

Claramente, $|\mathbb{Z}_{pq}^*| = |\mathbb{Z}_p^*|\,|\mathbb{Z}_q^*|$, e como $\operatorname{mdc}(p, q) = 1$, o teorema chinês dos restos[15] determina que

$$f : \mathbb{Z}_{pq}^* \to \mathbb{Z}_p^* \times \mathbb{Z}_q^*,$$

dada por

$$f(x) = (x, x)$$

é bijetora.
Definimos agora dois conjuntos[16], ambos com metade do tamanho de $\mathbb{Z}_{pq}^*$:

$$E = \left\{1 < x < \frac{pq}{2}\right\} \qquad D = \left\{(a, b) : 1 < a < p,\ \ 1 < b < \frac{q}{2}\right\}$$

Os dois conjuntos tem o mesmo tamanho, mas no conjunto D mantivemos

[13] George Rousseau, matemático do Século XX. Não é Jean-Jacques Rousseau (1712-1778), filósofo e teórico político, que já não estava mais vivo quando Gauss elaborou a primeira demonstração do teorema.

[14] A apresentação de Rousseau é bem mais compacta que a nossa – o corpo da demonstração tem seis parágrafos.

Rousseau, G. On the Quadratic Reciprocity Law. **Journal of the Australian Mathematical Society**, v. 51, p. 423–425, 1991.

[15] **Teorema 6.18:** A função f (definida na equação 6.5) dada por

$$f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$$
$$f(x) = (x, x),$$

com $\operatorname{mdc}(m, n) = 1$, é bijetora.

[16] Como p, q são primos **ímpares**, $(q-1)/2,\ (pq-1)/2\ \in \mathbb{Z}$ são os maiores valores em cada conjunto.

os valores $1, \ldots p-1$ para a, e reduzimos os valores de b para $1, \ldots \frac{q-1}{2}$ – o que reduz o tamanho do conjunto pela metade!

Ainda temos uma bijeção: para cada $x \in E$, há um único par $\pm(a, b)$. Desta forma, temos que o produto dos pares (x, x), com $x \in E$ deve ser idêntico ao produto dos pares $(a, b) \in D$.

$$\prod_{x \in E} (x, x) = \pm \prod_{(a,b) \in D} (a, b), \tag{9.1}$$

onde o produtório é módulo p e q:

$$\left(\prod x \pmod p, \prod x \pmod q\right),$$
$$\left(\prod a \pmod p, \prod b \pmod q\right).$$

No produtório dos pares (a, b), no lado esquerdo do par haverá o produto dos valores de a entre 1 e $p-1$ (portanto $(p-1)!$), repetido $(q-1)/2$ vezes, portanto igual a

$$\begin{aligned} &(p-1)!^{\frac{q-1}{2}} \\ \equiv &(-1)^{\frac{q-1}{2}} \pmod p. \end{aligned} \qquad \text{(Teorema de Wilson [17])}$$

No lado direito do produtório desses pares, os valores multiplicados são $1, 2, \ldots, (q-1)/2$, repetidos $p-1$ vezes:

$$\left[\left(\frac{q-1}{2}\right)!\right]^{p-1}$$

Mas

$$\begin{aligned} -1 &\equiv (q-1)! && \text{(Teorema de Wilson)} \\ &\equiv \left[(1)(2)\cdots\left(\frac{q-1}{2}\right)\right]\left[(-1)(-2)\cdots\left(-\frac{q-1}{2}\right)\right] \\ &\equiv (-1)^{\frac{q-1}{2}}\left(\frac{q-1}{2}\right)!^2 \pmod q \end{aligned}$$

[17] **Teorema 6.9 (de Wilson):** p é primo se e somente se $(p-1)! \equiv -1 \pmod p$.

E portanto,

$$\begin{aligned}\left[\left(\frac{q-1}{2}\right)!\right]^{p-1} &\equiv \left\{\left[\left(\frac{q-1}{2}\right)!\right]^2\right\}^{\frac{p-1}{2}} \\ &\equiv \left[-(-1)^{\frac{q-1}{2}}\right]^{\frac{p-1}{2}} \\ &\equiv (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \pmod q.\end{aligned}$$

O produtório é, portanto

$$\prod_{(a,b)\in D}(a,b) = \prod_{\substack{a\le p-1\\ b\le(q-1/2)}} = \left((-1)^{\frac{q-1}{2}},\ (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right). \tag{9.2}$$

O conjunto E tem a primeira metade de $\mathbb{Z}_{pq}$, e vemos que

$$\mathbb{Z}_{pq} = E \cup -E.$$

Se $\mathbb{Z}_{pq}$ contém q vezes a sequência $1\cdots p$ (módulo pq), então E contém metade delas, ou seja, $(q-1)/2$ sequências e mais meia sequência:

$$\frac{q-1}{2}p + \frac{p}{2} = \underbrace{\frac{pq}{2}}_{\substack{\text{tamanho}\\ \text{de } \mathbb{Z}_{pq}}}.$$

Calculamos o produtório de E, inicialmente usando módulo p:

$$\begin{aligned}\prod_{x\in P} x &\equiv \frac{\left[(p-1)!\right]^{\frac{q-1}{2}}\left(\frac{p-1}{2}\right)!}{q^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!} && \pmod p \\ &\equiv (-1)^{\frac{q-1}{2}}\frac{\left(\frac{p-1}{2}\right)!}{q^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!} && \pmod p && \text{(T. Wilson)} \\ &\equiv (-1)^{\frac{q-1}{2}}\left(q^{\frac{p-1}{2}}\right)^{-1} && \pmod p && \text{(simplificando)} \\ &\equiv (-1)^{\frac{q-1}{2}}q^{\frac{p-1}{2}} && \pmod p && \text{(inverso de } \pm 1 \text{ é ele mesmo)} \\ &\equiv (-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) && \pmod p && \text{(crit. Euler}^{18}\text{)}\end{aligned}$$

Por simetria, o mesmo ocorre módulo q, e temos os seguintes dois fatos:

$$\begin{aligned}\prod_{x\in P} x &\equiv (-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) \pmod{p}\\ &\equiv (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) \pmod{q}\end{aligned}$$

Temos agora o produtório de E:

$$\prod_{x\in E}(x,x) = \left((-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right),\ (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right)\right) \tag{9.3}$$

Finalmente, dividimos 9.3 por 9.2, obtendo $(1,1)$:

$$\begin{aligned}(1,1) &= \frac{\prod_{x\in E}(x,x)}{\prod_{(a,b)\in D}(a,b)}\\ &= \left(\frac{(-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right)}{(-1)^{\frac{q-1}{2}}},\quad \frac{(-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right)}{(-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}}}\right)\\ &= \left[\left(\frac{q}{p}\right),\ (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)\right].\end{aligned}$$

Como os dois lados do par são iguais a um,

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right),$$

que é o enunciado da Lei da Reciprocidade Quadrática (usamos igualdade, "$=$", ao invés de congruência, "$\equiv$", porque os números são todos iguais a ± 1, congruentes, módulo p e módulo q). □

9.2.3 Demonstração Geométrica de Eisenstein

Nesta seção detalharemos a demonstração geométrica dada por Eisenstein[19], que é provavelmente uma das mais simples (é elementar e transparente). A demonstração é uma simplificação da terceira demonstração de Gauss. Para esta demonstração, Eisenstein formulou um Lema, não muito diferente de outro, proposto por Gauss.

[18] **Teorema 9.1 (critério de Euler)**: Se p é primo, então a é resíduo quadrático módulo p se e somente se

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

[19] Ferdinand Gotthold Max Eisenstein (1823-1852), Alemão.

Definição 9.3. $\mathrm{LR}_m(x)$ *é o menor representante positivo da classe de equivalência de* x *módulo* m*:*

$$\mathrm{LR}_m(x) = \text{menor } a \text{ em } [0, m) \text{ tal que } a \equiv x \pmod{m}. \qquad \blacktriangleleft$$

Exemplo 9.2. *Temos por exemplo* $3 \equiv 12 \equiv -6 \pmod 9$*, mas* $\mathrm{LR}_9(3) = \mathrm{LR}_9(12) = \mathrm{LR}_9(-6) = 3$*.* $\blacktriangleleft$

O Lema de Eisenstein estabelece uma relação importante entre dois primos p e q e o símbolo de Legendre (q/p).

Lema 9.4 (de Eisenstein)**.** *Seja* p *um primo ímpar e* q *um ímpar positivo. Então*

$$\left(\frac{q}{p}\right) = (-1)^{\sum \left\lfloor \frac{qu}{p} \right\rfloor},$$
$$\text{com } u = 2, 4, 6, \ldots, p-1$$

Exemplo 9.3.

$$\begin{aligned}\left(\frac{5}{11}\right) &= (-1)^{\lfloor \frac{2\cdot5}{11} \rfloor \lfloor \frac{4\cdot5}{11} \rfloor \lfloor \frac{6\cdot5}{11} \rfloor \lfloor \frac{8\cdot5}{11} \rfloor \lfloor \frac{10\cdot5}{11} \rfloor} \\ &= (-1)^{\lfloor \frac{10}{11} \rfloor \lfloor \frac{20}{11} \rfloor \lfloor \frac{30}{11} \rfloor \lfloor \frac{40}{11} \rfloor \lfloor \frac{50}{11} \rfloor} \\ &= (-1)^{0+1+2+3+4} \\ &= +1.\end{aligned}$$

De fato, 5 *é resíduo quadrático módulo* 11*, já que* $4^2 = 16 \equiv 5 \pmod{11}$*.* $\blacktriangleleft$

Exemplo 9.4. *Escolhemos desta vez* 7 *módulo* 13*:*

$$\begin{aligned}\left(\frac{7}{13}\right) &= (-1)^{\lfloor \frac{2\cdot7}{13} \rfloor + \lfloor \frac{4\cdot7}{13} \rfloor + \lfloor \frac{6\cdot7}{13} \rfloor + \lfloor \frac{8\cdot7}{13} \rfloor + \lfloor \frac{10\cdot7}{13} \rfloor + \lfloor \frac{12\cdot7}{13} \rfloor} \\ &= (-1)^{\lfloor \frac{14}{13} \rfloor + \lfloor \frac{28}{13} \rfloor + \lfloor \frac{42}{13} \rfloor + \lfloor \frac{56}{13} \rfloor + \lfloor \frac{70}{13} \rfloor + \lfloor \frac{84}{13} \rfloor} \\ &= (-1)^{1+2+3+4+5+6} \\ &= (-1)^{21} \\ &= -1.\end{aligned}$$

E 7 não *é resíduo quadrático módulo* 13*.* $\blacktriangleleft$

A demonstração dada aqui é a mesma de Eisenstein, com a simplificação de notação sugerida por Gauss, que observou que o menor inteiro positivo representando $qu \pmod p$ é $\left\lfloor \frac{qu}{p} \right\rfloor$.

Demonstração. Observando o somatório $\sum \left\lfloor \frac{qu}{p} \right\rfloor$, vemos que será útil defi-

nir

$$r(u) = LR_p(qu),$$

a classe de equivalência módulo p no numerador.
Primeiro, notamos que

$$r(u)$$

é par, porque $u = 2k$ (ou seja, u é par), logo $r(u) \equiv (2k)q \pmod{p}$.
Além disso,

$$(-1)^{r(u)} r(u) \pmod{p}$$

é também par.
Agora observamos também que os $(-1)^{r(u)} r(u)$ são todos distintos módulo p. Suponha que existam u e t, tais que $(-1)^{r(u)} r(u) \equiv (-1)^{r(t)} r(t) \pmod{p}$. Então teríamos

$$\begin{aligned}
(-1)^{r(u)} r(u) &\equiv (-1)^{r(t)} r(t) \pmod{p} \\
\pm r(u) &\equiv r(t) \pmod{p} \\
\pm qu &\equiv qt \pmod{p} \\
\pm u &\equiv t \pmod{p} \\
r(u) &= r(t).
\end{aligned}$$

Há $(p-1)/2$ valores diferentes para $(-1)^{r(u)} r(u)$, porque o somatório foi definido para $u = 2, 4, 6, p-1$. Como são todos distintos módulo p, eles devem portanto ser (módulo p) uma permutação da sequência $2, 4, 6, \ldots, p-1$.
Calculamos

$$\begin{aligned}
\prod r(u) &\equiv \prod qu \\
&\equiv 2q \cdot 4q \cdot 6q \cdots (p-1)q \\
&\equiv q^{\frac{p-1}{2}} \prod u \pmod{p}.
\end{aligned}$$

Mas como os $(-1)^{r(u)} r(u)$ são permutação de $2, 4, 6, \ldots, p-1$ módulo p,

$$\begin{aligned}
\prod u &\equiv \prod (-1)^{r(u)} r(u) \\
\prod u &\equiv (-1)^{\sum r(u)} \prod r(u) \\
\prod u &\equiv (-1)^{\sum r(u)} q^{\frac{p-1}{2}} \prod u \\
1 &\equiv (-1)^{\sum r(u)} q^{\frac{p-1}{2}} \\
(-1)^{\sum r(u)} &\equiv q^{\frac{p-1}{2}} \\
(-1)^{\sum r(u)} &\equiv \left(\frac{q}{p}\right) \pmod{p}.
\end{aligned}$$

Ao analisar a demonstração de Eisenstein, Gauss observou que

$$\frac{qu}{p} = \left\lfloor \frac{qu}{p} \right\rfloor + \frac{r(u)}{p},$$

q é ímpar e u é par, temos

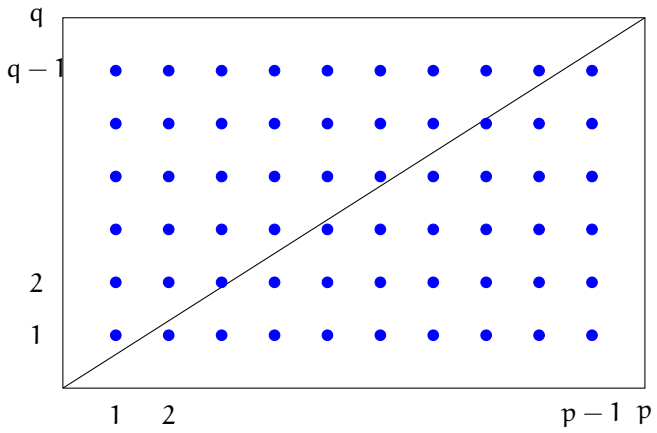
$$\left\lfloor \frac{qu}{p} \right\rfloor \equiv r(u) \pmod 2.$$

Assim,

$$\left(\frac{q}{p}\right) = (-1)^{\sum \left\lfloor \frac{qu}{p} \right\rfloor}. \qquad \square$$

Passamos agora à demonstração da Lei da Reciprocidade Quadrática.

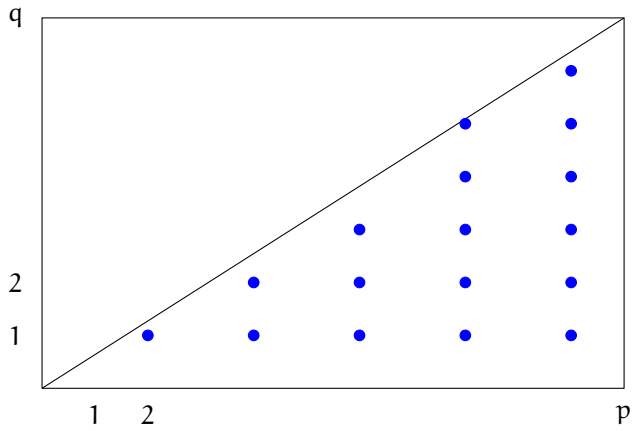
Demonstração. (da Lei da Reciprocidade Quadrática) Observamos, no plano Cartesiano, o retângulo delimitado entre a origem e o ponto (p, q). A diagonal é dada pela reta $y = qx/p$.



Inicialmente observamos que:

- cada coluna tem um número par de pontos inteiros (que são os de ordenada $1, 2, \ldots, q-1$).
- não há pontos sobre a diagonal, que é definida pela reta $y = qx/p$, porque sendo p e q primos e $x < p$, qx/p não é inteiro.

Note que a quantidade de pontos nas colunas **pares** abaixo da diagonal é $\lfloor \frac{2q}{p} \rfloor$, $\lfloor \frac{4q}{p} \rfloor$, ..., $\lfloor \frac{(p-1)q}{p} \rfloor$.



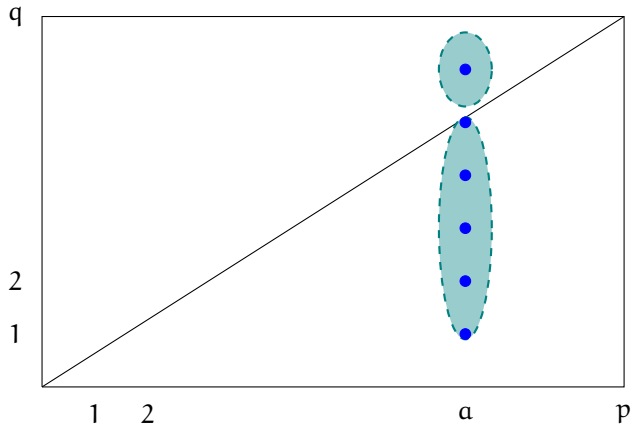
Assim, a soma de pontos nas colunas pares abaixo da diagonal é

$$d = \left\lfloor \frac{2q}{p} \right\rfloor + \left\lfloor \frac{4q}{p} \right\rfloor + \ldots + \left\lfloor \frac{(p-1)q}{p} \right\rfloor,$$

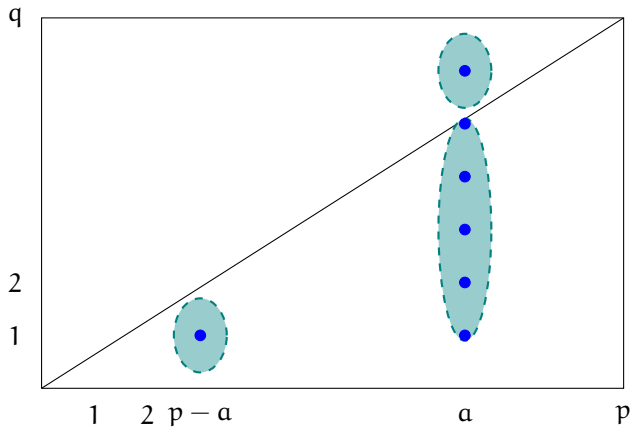
exatamente o expoente no lema de Eisenstein. Podemos portanto concluir que

$$\left(\frac{p}{q}\right) = (-1)^d.$$

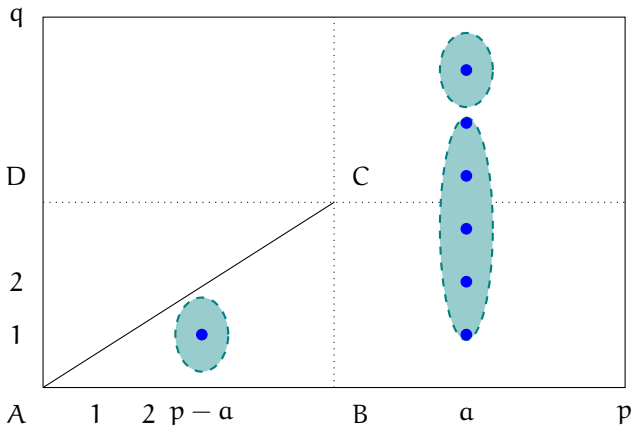
Como a quantidade total de pontos em cada coluna é par, a quantidade de pontos *acima* da diagonal, em cada coluna, deve ter a mesma paridade que a quantidade de pontos *abaixo* dela. A próxima figura mostra uma abscissa a e os pontos inteiros de a acima e abaixo da diagonal.



No entanto, a quantidade de pontos *acima* da diagonal na coluna a é a mesma que a quantidade *abaixo* da diagonal na coluna $p-a$. Isto é ilustrado na próxima figura. Note que, como p é ímpar e a é par, $p-a$ é ímpar.



Na figura acima, as três regiões marcadas (três trechos de colunas) tem quantidades de pontos inteiros com a mesma paridade. Observamos também que há uma correspondência um-para-um entre a quantidade de pontos na abscissa a acima da diagonal e a quantidade de pontos da abscissa $p - a$, abaixo da diagonal.
A seguir dividimos o retângulo ao meio, na horizontal e na vertical, obtendo um novo retângulo $ABCD$.



A paridade da quantidade total de pontos **com abscissa par** abaixo da diagonal em $ABCD$ (que chamamos de d) é a mesma que a da quantidade **total** de pontos no triângulo ABC, que chamamos de α:

$$\sum \left\lfloor \frac{qu}{p} \right\rfloor \equiv \alpha \pmod 2.$$

Para verificar que isto vale, observamos que ao contar as paridades das colunas com abscissa par abaixo da diagonal, contamos as colunas pares

dentro de ABC, e também as colunas pares após B – mas para cada uma dessas, há uma coluna ímpar em ABC.
Com este resultado, chegamos de imediato a

$$\left(\frac{q}{p}\right) = (-1)^{\alpha}.$$

Trocando os papéis de q e p, e denotando a quantidade de pontos em ACD por β, obtemos também

$$\left(\frac{p}{q}\right) = (-1)^{\beta}.$$

Ou seja,

$$\left(\frac{q}{p}\right)\left(\frac{q}{p}\right) = (-1)^{\alpha}(-1)^{\beta}$$

Mas a soma das quantidades de pontos nos dois triângulos é

$$\alpha + \beta = \frac{(p-1)}{2}\frac{(q-1)}{2},$$

o que nos dá imediatamente a Lei da Reciprocidade Quadrática:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\alpha}(-1)^{\beta} = (-1)^{(p-1)(q-1)/4}. \qquad \square$$

9.2.4 Demonstração de Gauss (a quarta, usando raízes da unidade)

A demonstração a seguir usa raízes da unidade, e portanto identifica uma relação entre a lei da reciprocidade quadrática e diversas outros conceitos (polígonos construtíveis com régua e compasso, por exemplo).
A apresentação dada é inspirada naquela dada por Jay Goldman[20]. O Teorema é provado não somente para p, q primos, mas para p, q ímpares (o símbolo de Legendre é usado, mas o uso que é feito dele permite que seja lido como símbolo de Jacobi).
Antes de começar, é interessante repetir a definição de raiz da unidade (Definição 7.10. na página 188, Capítulo 7).
Definição 7.10 (raiz da unidade): Uma **raiz da unidade** (ou ainda, **n-ésima raiz da unidade**) é um número $z \in \mathbb{C}$ tal que $z^n = 1$.
As n-ésimas raízes da unidade formam um grupo, conforme o Teorema 7.22[21].

[20] **Goldman**, Jay R. **The Queen of Mathematics: A Historically Motivated Guide to Number Theory**. Natick, MA: A. K. Peters, 1998.
Pag 212.

[21] **Teorema 7.22:** Fixado n, as raízes da unidade formam um grupo.

Lema 9.5. *Seja $z \in \mathbb{C}$ e p um primo ímpar. Então*

$$\sum_{t=0}^{p-1} \zeta^{zt} = \begin{cases} p & \text{se } p \mid z \\ 0 & \text{caso contrário.} \end{cases}$$

Demonstração. Se $p \mid z$, então $\zeta^{zt} = \zeta^{(kp)t} = \zeta^0 = 1$, e o somatório é evitentemente igual a p.
Se $p \nmid z$, então

$$\sum_{t=0}^{p-1} \zeta^{zt} = \frac{\zeta^{zp} - 1}{\zeta^z - 1} = 0,$$

porque $\zeta^{zp} = 1$. □

Somas de Gauss são somatórios de raízes da unidade, de grande importância em diferentes áreas de Teoria de Números. Aqui apresentamos somente uma forma simples de soma de Gauss; há muitas outras generalizações.

Definição 9.4 (soma de Gauss)**.** *Se p é um primo ímpar $k \in \mathbb{Z}$ e ζ é uma p-ésima raiz da unidade, então a **soma de Gauss**, denotada por g_k, é*

$$g_k = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^{kt}.$$

Também denotamos

$$g = g_1.$$ ◀

Exemplo 9.5. *Sejam $p = 3$ e $\zeta = e^{2i\pi/3}$. Então, fixados ζ e p, escolhemos $k = 2$ e*

$$\begin{aligned} g_2 &= \sum_{t=0}^{2} \left(\frac{t}{p}\right) \zeta^t \\ &= \left(\frac{0}{3}\right) \zeta^0 + \left(\frac{1}{3}\right) \zeta^{1(2)} + \left(\frac{2}{3}\right) \zeta^{2(2)} \\ &= 0\zeta^0 + 1\zeta^2 - 1\zeta^4 \\ &= 0 + (e^{2i\pi/3})^2 - (e^{2i\pi/3})^4 \\ &= \left(\frac{-1 + i\sqrt{3}}{2}\right)^2 - \left(\frac{-1 + i\sqrt{3}}{2}\right)^4 \\ &= -i\sqrt{3}. \end{aligned}$$ ◀

Lema 9.6.

$$g_k = \left(\frac{k}{p}\right) g.$$

Demonstração. Se $p \mid k$, então os dois lados da equação são zero. O lado esquerdo é:

$$\begin{aligned} g_k &= \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^{kt} \\ &= \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) 1, \end{aligned}$$

mas como a quantidade de resíduos quadráticos e não quadráticos módulo p é a mesma, os termos (t/p) se anulam.
O lado direito é

$$\left(\frac{k}{p}\right) g,$$

mas como $p \mid k$, o símbolo de Legendre (k/p) é sempre zero.
Consideramos agora o caso em que $p \nmid k$. Então (k/p) será sempre $+1$ ou -1, e

$$\left(\frac{k}{p}\right)^2 = 1.$$

Assim,

$$\begin{aligned} g_k &= \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^{kt} \\ &= \left(\frac{k}{p}\right)^2 \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^{kt} && \text{(multiplicando por } 1 = (k/p)^2\text{)} \\ &= \left(\frac{k}{p}\right) \sum_{t=0}^{p-1} \left(\frac{kt}{p}\right) \zeta^{kt} && \text{(propriedade do símbolo de Legendre)} \\ &= \left(\frac{k}{p}\right) \sum_{r=0}^{p-1} \left(\frac{r}{p}\right) \zeta^{r} && (9.4) \\ &= \left(\frac{k}{p}\right) g. \end{aligned}$$

A passagem 9.4 é válida porque como $\{0, 1, \ldots, p-1\}$ é sistema de resíduos, $\{0, k, 2k, \ldots, kp-1\}$ também é, e os representantes das classes de congruência módulo p serão os mesmos. □

Seja

$$p^* = (-1)^{(p-1)/2} p.$$

Assim como na seção 9.2.1, esta definição resulta que p^* será igual a p, mas com sinal $+1$ se p é da forma $4k+1$ ou sinal -1 se p é da forma $4k+3$.

Também é verdade que

$$p^* = \left(\frac{-1}{p}\right) p = (-1)^{(p-1)/2} p.$$

Exemplo 9.6. *A tabela a seguir ilustra* p^* *e sua relação com* $(-1/p)$.

p	forma	$-1 \pmod p$	$\sqrt{-1} \pmod p$	$(-1/p)$	p^*
101	$4k+1$ $(k=25)$	100	10	$+1$	101
23	$4k+3$ $(k=5)$	22	$\nexists$	-1	-23

◀

Teorema 9.9. *Se* $p \nmid k$*, então* $g^2 = p^*$.

Demonstração. Escrevemos $\sum_{t=0}^{p-1} g_k g_{-k}$ de duas maneiras diferentes.

Primeiro, se $p \nmid k$, então

$$g_k g_{-k} = \left(\frac{k}{p}\right)\left(\frac{-k}{p}\right) g^2 = \left(\frac{-1}{p}\right) g^2,$$

independente de t. Se $p \mid k$, $g_k = 0$. Então Assim,

$$\begin{aligned} \sum_{t=0}^{p-1} g_k g_{-k} &= (p-1) g_k g_{-k} \\ &= (p-1)\left(\frac{-1}{p}\right) g^2. \end{aligned} \tag{9.5}$$

ou seja, $p-1$ vezes o valor de $g_k g_{-k}$ (o somatório tem p termos, mas um deles é com $t = 0$).

Escrevemos a soma novamente.

$$g_k g_{-k} = \sum_a \sum_b \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \zeta^{k(a-b)},$$

onde a e b variam entre 0 e $p-1$.

$$\begin{aligned} \sum_k g_k g_{-k} &= \sum_a \sum_b \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \sum_k \zeta^{k(a-b)} \\ &= \sum_a \sum_b \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \delta(a,b) \\ &= (p-1)p. \end{aligned} \tag{9.6}$$

Aqui $\delta(a,b)$ é a o δ de Kronecker, $\delta(a,b) = 1$ se $a = b$, e $\delta(a,b) = 0$ se $a \neq b$.

Os lados direitos em 9.5 e 9.6 são iguais, portanto escrevemos

$$\begin{aligned}(p-1)\left(\frac{-1}{p}\right)g^2 &= (p-1)p\\ \left(\frac{-1}{p}\right)g^2 &= p\\ \left(\frac{-1}{p}\right)^2 g^2 &= \left(\frac{-1}{p}\right)p\\ g^2 &= \left(\frac{-1}{p}\right)p, \qquad ((\pm 1)^2 = +1)\end{aligned}$$

e a demonstração está completa. □

Corolário 9.3. *Seja* p *um primo ímpar.*
Se $p = 4k+1$ *então* $g = \pm\sqrt{+p}$*, e* $g^2 = p$*.*
Se $p = 4k+3$ *então* $g = \pm\sqrt{-p}$*, e* $g^2 = -p$*.*
As operações são todas módulo p*.*

Até este ponto, Gauss tinha uma forma fechada para o *quadrado* da soma (g^2), mas não sabia qual das duas raizes quadradas era o valor de g – ou seja, faltava determinar o sinal da soma de Gauss, g. Depois de muito tempo, Gauss finalmente chegou a uma demonstração. O Teorema 9.10 determina o sinal da soma de Gauss. A demonstração será omitida.

Teorema 9.10. *Para qualquer primo ímpar* p*,*

$$\begin{aligned}g &= \sqrt{p} \quad \text{se } p = 4k+1,\\ g &= i\sqrt{p} \quad \text{se } p = 4k+3.\end{aligned}$$

Como a Lei da Reciprocidade Quadrática trata de mais de um número primo, fará sentido explicitarmos o primo na soma de Gauss, como um argumento. Denote

$$g_k(r) = \sum_{t=0}^{r-1}\left(\frac{t}{r}\right)\zeta^{kt},$$

onde ζ é r-ésima raiz primitiva da unidade.
Os Lemas 9.7 e 9.8 são usados na demonstração da reciprocidade quadrática. As demonstrações não são difíceis, e são pedidas nos Exercícios 277 e 278.

Lema 9.7.

$$g_k(r) = \left(\frac{k}{r}\right)g_1(r)$$

Lema 9.8. *Se* p, q *são primos ímpares distintos, então*

$$g_p(q)g_q(p) = g_1(pq),$$

com raízes da unidade distintas no cômputo das somas de Gauss (em g_p *usa-se* p*-ésima, e em* g_q *usa-se* q*-ésima).*

Demonstração. (da Lei da Reciprocidade Quadrática)
Os Lemas 9.7 e 9.8 nos permitem escrever

$$\left(\frac{q}{p}\right) g_1(p) \left(\frac{p}{q}\right) g_1(q) = g_1(pq).$$

Mas

$$g = i^{\left(\frac{p-1}{2}\right)^2} \sqrt{p},$$

portanto reescrevemos

$$\begin{aligned}
\left(\frac{q}{p}\right) g_1(p) \left(\frac{p}{q}\right) g_1(q) &= g_1(pq) \\
\left(\frac{q}{p}\right) \left(\frac{p}{q}\right) &= \frac{g_1(pq)}{g_1(p) g_1(q)} \\
&= i^{\left(\frac{pq-1}{2}\right)^2 - \left(\frac{p-1}{2}\right)^2 - \left(\frac{q-1}{2}\right)^2} \\
&= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.
\end{aligned}$$

□

A sexta demonstração de Gauss para este Teorema usa as mesmas idéias, mas evita o problema de calcular a soma de Gauss e o uso direto de números complexos, trabalhando com polinômios módulo p.

9.3 Método para resolução de congruências quadráticas

Voltamos a atenção agora para a obtenção de um método para determinar as raízes quadradas de a (as soluções para $x^2 \equiv a \pmod{p}$).

9.3.1 Módulo primo

Quando $p = 4k+3$ é bastante simples resolver equações quadráticas módulo p. Tratamos somente deste caso.

Teorema 9.11. *Seja* $p = 4k+3$ *primo,* a *um resíduo quadrático módulo* p*. Então* $x \equiv a^{k+1} \pmod{p}$ *é solução para* $x^2 \equiv a \pmod{p}$*.*

Demonstração.

$$\begin{aligned} x^2 &\equiv \left(a^{k+1}\right)^2 \\ &\equiv a^{2k+2} \\ &\equiv a^{2k+1}a \\ &\equiv a^{\frac{p-1}{2}}a && \text{(porque } p = 4k+3\text{)} \\ &\equiv a \pmod{p}. && \text{(critério de Euler)} \end{aligned}$$

Pudemos usar o critério de Euler no último passo porque já sabemos que a é resíduo quadrático. Assim, uma solução para $x^2 \equiv a \pmod{p}$ é a classe de congruências $a^{k+1} \pmod{p}$ – se p for da forma $4k+3$. □

Escolhemos para exemplo o módulo $11 = 4(2)+3$. Pelo critério de Euler, 3 é resíduo quadrático módulo 11:

$$3^{\frac{11-1}{2}} \equiv 3^5 \equiv 243 \equiv 1 \pmod{11}.$$

A raiz quadrada de 3 módulo 11 é

$$3^{k+1} \equiv 3^3 \equiv 27 \equiv 5 \pmod{11}.$$

Verificamos:

$$5^2 \equiv 25 \equiv 3 \pmod{11}. \tag{9.7}$$

9.3.2 Módulo potência de primo

Sabemos calcular as raízes quadradas de um número módulo p primo, mas não módulo potência de primo. O Teorema 9.12 é uma variante do Lema de Hensel (Lema 6.7). Ele nos permite usar as raízes módulo p para determinar as raízes p^k: se $x^2 \equiv a \pmod{p}$, então existe algum y tal que $y^2 \equiv a \pmod{p^k}$.

Teorema 9.12. *Seja p um primo ímpar. Se $x^2 \equiv a \pmod{p^k}$, então para qualquer $m \leq k$,*

$$y^2 \equiv a \pmod{p^{m+k}},$$

com

$$\begin{aligned} y &= x + tp^k, \\ t &= -\frac{x^2-a}{2xp^k} \pmod{p^m}. \end{aligned}$$

Exemplificamos a seguir. Sabemos que $(\pm 7)^2 \equiv 4 \pmod{5}$, e como $3 \equiv -7$

$(\mathrm{mod}\ 5)$, $3, 7$ são soluções para $x^2 \equiv 4\ (\mathrm{mod}\ 5)$:

$$\begin{aligned} 7^2 &\equiv 49 \equiv 4 \pmod 5 \\ (-7)^2 \equiv (3)^2 &\equiv 9 \equiv 4 \pmod 5 \end{aligned}$$

Partindo das soluções $3, 7$ para módulo 5 obteremos soluções para módulo 5^3. Queremos resolver

$$y^2 \equiv 4 \pmod{5^{1+2}},$$

logo

$$\begin{aligned} y &= 3 + t5, \\ t &\equiv -\frac{3^2 - 4}{2(3)5} \pmod{5^2}. \end{aligned}$$

Calculamos t:

$$t \equiv -\frac{5}{6(5)} \equiv -(6)^{-1} \equiv -126 \equiv 24 \pmod{25}.$$

Finalmente, obtemos y (uma raiz quadrada de 4 módulo 5^3):

$$y = 3 + 24(5) = 123.$$

Verificamos que

$$123^2 \equiv 15129 \equiv 4 \pmod{5^3}.$$

9.3.3 Módulo composto

Quando o módulo é composto, podemos usar as soluções módulo p para cada primo p na fatoração do módulo na construção de uma solução.

Lema 9.9. *Se p está na fatoração de m com expoente k (ou seja, $m = \cdots p^k \cdots$), e $x^2 \equiv y\ (\mathrm{mod}\ m)$, então $x^2 \equiv y\ (\mathrm{mod}\ p^k)$.*

Demonstração.

$$\begin{aligned} &x^2 \equiv y \pmod m \\ &m \mid x^2 - y \\ &p^k \mid x^2 - y && \text{(porque } p^k | m\text{)} \\ &x^2 \equiv y \pmod{p^k} && \square \end{aligned}$$

Suponha que queiramos resolver $x^2 = y\ (\mathrm{mod}\ pq)$. Calculamos $\pm x\ (\mathrm{mod}\ p)$, $\pm x\ (\mathrm{mod}\ q)$, e depois obtemos as raízes quadradas módulo pq usando o Teorema Chinês dos Restos para resolver quatro sistemas (listados um por linha):

$$\begin{array}{llllll}
(1) & x \equiv & r_1 & \pmod{p}, & x \equiv & r_2 \pmod{q} \\
(2) & x \equiv & -r_1 & \pmod{p}, & x \equiv & r_2 \pmod{q} \\
(3) & x \equiv & r_1 & \pmod{p}, & x \equiv & -r_2 \pmod{q} \\
(4) & x \equiv & -r_1 & \pmod{p}, & x \equiv & -r_2 \pmod{q}
\end{array}$$

Exemplo 9.7. *Sejam* $p = 11, q = 19$*. Encontraremos as raízes quadradas de* 5 *módulo* $pq = 209$*.*
Vemos que $11 = 4(2) + 3$*, e uma das raízes quadradas é* $5^{2+1} \equiv 125 \equiv 4 \pmod{11}$*. A outra é* $-4 \equiv 7 \pmod{11}$*.*
Para $19 = 4(4) + 3$*, uma solução é* $x = 5^5 = 3125 \equiv 9 \pmod{19}$*. A outra é* $-9 \equiv 10 \pmod{19}$*.*
Agora resolvemos os quatro sistemas,

$$\begin{array}{llllll}
(1) & x \equiv & 4 & \pmod{11}, & x \equiv & 9 \pmod{19} \\
(2) & x \equiv & 4 & \pmod{11}, & x \equiv & 10 \pmod{19} \\
(3) & x \equiv & 7 & \pmod{11}, & x \equiv & 9 \pmod{19} \\
(4) & x \equiv & 7 & \pmod{11}, & x \equiv & 10 \pmod{19}
\end{array}$$

As soluções são $180, 48, 161$ *e* 29*.* ◀

9.3.4 Equação geral do segundo grau

Determinar se a equação de segundo grau $ax^2 + bx + c \equiv 0 \pmod{m}$ tem soluções é equivalente a determinar se a equação $y^2 \equiv \Delta \pmod{m}$, onde $\Delta = b^2 - 4ac$, tem solução, já que

$$\begin{aligned}
x &\equiv \frac{-b \pm \sqrt{\Delta}}{2a} && \pmod{m} \\
2ax + b &\equiv \pm\sqrt{\Delta} && \pmod{m} \\
(2ax + b)^2 &\equiv \Delta && \pmod{m} \\
y^2 &\equiv \Delta && \pmod{m}
\end{aligned}$$

Isto vale desde que $\mathrm{mdc}\,(2a, m) = 1$ (porque usamos a lei do cancelamento, multiplicando os dois lados por $2a$). Quando o módulo é primo, $2a$ será evidentemente co-primo com o módulo.
Resolveremos agora $x^2 - 6x + 5 \equiv 0 \pmod{11}$. Temos

$$\Delta = b^2 - 4ac = 36 - 20 = 16 \equiv 5 \pmod{11}.$$

O critério de Euler nos garante que 5 é resíduo quadrático módulo 11, conforme já calculamos na seção anterior (equação9.7). A raiz de Δ é, portanto,

$$5^{k+1} \equiv 5^3 \equiv 125 \equiv 4 \pmod{11}.$$

Podemos simplesmente calcular

$$\begin{aligned}
(2ax+b)^2 &\equiv \Delta && \pmod{11}\\
2ax+b &\equiv 4 && \pmod{11}\\
2x-6 &\equiv 4 && \pmod{11}\\
2x &\equiv 10 && \pmod{11}\\
x &\equiv 5 && \pmod{11}
\end{aligned}$$

Por último, fazemos uma verificação:

$$\begin{aligned}
x^2-6x+5 &\equiv (5)^2-6(5)+5 && \pmod{11}\\
&\equiv 25-30+5 && \pmod{11}\\
&\equiv 0 && \pmod{11}
\end{aligned}$$

Exercícios

Ex. 252 — Calcule:

$$\left(\frac{21}{11}\right),\quad \left(\frac{31}{3}\right),\quad \left(\frac{122}{23}\right),\quad \left(\frac{119}{7}\right).$$

Ex. 253 — Resolva (deixe potências indicadas, não é necessário reduzir as classes de congruência), ou explique porque não é possível:

$$\begin{aligned}
x^2 &\equiv 10 && \pmod{43}\\
X^2 &\equiv 5 && \pmod{31}\\
3x^2-x+1 &\equiv 0 && \pmod{19}\\
x^2-x+4 &\equiv 0 && \pmod{29}\\
2x^2-10 &\equiv 0 && \pmod{23}\\
3x^2-5 &\equiv 0 && \pmod{18}\\
4x^2-5 &\equiv 0 && \pmod{25}
\end{aligned}$$

Ex. 254 — Prove que quando m é ímpar,

$$\left(\frac{a}{m}\right)\left(\frac{b}{m}\right)=\left(\frac{ab}{m}\right).$$

Ex. 255 — Um resíduo quadrático módulo p pode ser raiz primitiva módulo pq, com p e q primos?

Ex. 256 — Seja p primo da forma $4k+1$. Determine a soma dos resíduos quadráticos módulo p contidos em $[1, p)$.

Ex. 257 — Quantos resíduos quadráticos existem módulo m, onde $m = pq$, com p, q primos?

Ex. 258 — Prove que se p e q são primos ímpares tais que existe um x inteiro positivo tal que $p = q + 4x$, então

$$\left(\frac{x}{p}\right) = \left(\frac{x}{q}\right).$$

Ex. 259 — Prove que todo primo p maior que 3 divide a soma de seus resíduos quadráticos; e que todo primo p maior que 5 divide a soma dos quadrados de seus resíduos quadráticos.

Ex. 260 — Prove o Lema 9.1.

Ex. 261 — Prove o Lema 9.2.

Ex. 262 — Prove o Coroário 9.2.

Ex. 263 — Usando o Lema 9.2, prove que há infinitos primos da forma $8k+7$.

Ex. 264 — Prove que há infinitos primos da forma $5k-1$.

Ex. 265 — Mostre que $|Q_n| = \phi(n)/R$, onde R é a quantidade de elementos em U_n tais que $x^2 = a$, sendo a um resíduo quadrático em U_n.

Ex. 266 — Prove que se n é um inteiro ímpar livre de quadrados, então existe $k \in \mathbb{Z}$ tal que $\operatorname{mdc}(k, n) = 1$ e $\left(\frac{k}{n}\right) = -1$.

Ex. 267 — Demonstre o Teorema 9.2.

Ex. 268 — Prove que a função $f : U_n \to Q_n$, tal que $f(x) = x^2$ é homomorfismo entre grupos.

Ex. 269 — Prove que se p é um primo ímpar e $a \neq 0$ um resíduo quadrático módulo p, então $-a$ é resíduo quadrático módulo p se e somente se $p = 4k+1$. (Use o resultado do Exercício 260).

Ex. 270 — Seja $m = pq$, com p e q primos ímpares. Se sortearmos um elemento $x \in \mathbb{Z}_m$, e verificarmos que seu símbolo de Jacobi é $+1$, qual é a probabilidade de x ser resíduo quadrático módulo m?

Ex. 271 — Prove a seguinte extensão do Teorema de Wilson: se p é primo

e $p \nmid a$, então

$$(p-1)! \equiv -\left(\frac{a}{p}\right) a^{\frac{p-1}{2}} \pmod{p}.$$

Ex. 272 — Prove que para n ímpar,

$$\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$$

Ex. 273 — Determine uma forma fechada para

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right),$$

quando a, b são inteiros ímpares.

Ex. 274 — Seja p um primo ímpar, e n o menor resíduo quadrático positivo módulo p. Prove que $n < 1 + \sqrt{p}$.

Ex. 275 — Determine se 17 é resíduo quadrático módulo 401.

Ex. 276 — Determine quais os primos p tais que 3 é resíduo quadrático módulo p.

Ex. 277 — Demonstre o Lema 9.7

Ex. 278 — Demonstre o Lema 9.8

Ex. 279 — Prove o Lema de Gauss:
Lema 9.10. *seja p primo e a coprimo com p; considere o conjunto $A = \{a, 2a, 3a, \ldots, [(p-1)/2]a\}$. Tome os menores representantes positivos dos elementos em A, módulo p. Seja n a quantidade desses $\mathrm{LR}_p(a_i)$ que são maiores que $p/2$:*

$$n = \left| \left\{ x \in A \ : \ \mathrm{LR}_p(X) > \frac{p}{2} \right\} \right|.$$

Então

$$\left(\frac{a}{p}\right) = (-1)^n.$$

Ex. 280 — Prove a Lei da Reciprocidade Quadrática usando o Lema de Gauss.

Ex. 281 — (Usando permutações) Em 1872, Yegor Ivanovich Zolotaryov (Его́р Ива́нович Золотарёв- o sobrenome é usualmente grafado "Zolotarev" no ocidente) provou[22] a Lei da Reciprocidade Quadrática usando o seguinte Lema.

[22] O artigo original é

Lema 9.11. *Seja* p *primo e* $a \in \mathbb{Z}$*, tal que* $p \nmid a$*. Seja também* τ *a permutação em* $\mathbb{Z}_p \setminus \{0\}$*, definida por*

$$\tau_a(k) = ak \pmod{p}$$

Então

$$\left(\frac{a}{p}\right) = \epsilon(\tau_a),$$

onde $\epsilon(\tau_a)$ *denota o sinal da permutação* τ_a*.*
Prove que o Lema de Zolotarev é equivalente ao Lema de Gauss (Lema 9.10).

Zolotareff, G. Nouvelle démonstration de la loi de réciprocité de Legendre. **Nouvelles Annales de Mathématiques**, v. 2, n. 11, p. 354–362, 1872.

O título se refere à "Lei de Reciprocidade de Legendre", que é como a Lei da Reprocidade Quadrática também era conhecida (Legendre chegou a formular uma demonstração incompleta). O enunciado do Lema de Zolotarev, no artigo (onde é um Teorema), é

> *Seja* p *um número primo ímpar. Dada uma sequência de números*
> *1)* $1, 2, 3, \ldots, p-1$
> *(· · ·)*
> ***Teorema I*** *– Seja* k *um número inteiro qualquer não divisível por* p*. O caracter da sequência*
> *3)* $k, 2k, 3k, \ldots, (p-1)k,$
> *se trocarmos os elementos por seus resíduos com respeito ao módulo* p*, que são encontrados na sequência (1), é igual a* $\left(\frac{k}{p}\right)$.

No original, em Francês,

> *Soît p un nombre premîer impair. Étant donnée une suite de nombres*
> *1)* $1, 2, 3, \ldots, p-1$
> *(· · ·)*
> ***Théorème I*** *– Soit* k *un nombre entier quelconeque non divisible par* p*. Le caractère de la suite*
> *3)* $k, 2k, 3k, \ldots, (p-1)k,$
> *si l'on y remplace les éléments par leurs résidus parrapport au module* p *qui se trouvent dans la série (1), est égal a* $\left(\frac{k}{p}\right)$.

As mais de trezentas demonstrações da Lei da Reciprocidade Quadrática podem ser agrupadas como variações de algumas poucas – e a de Zolotarev é uma delas. Curiosamente, a abreviação usada em referências é "G. Zolotareff"; a que consta no início do artigo é "M. Zolotareff"; e o nome, transliterado, é "Y. I. Zolotareff". Zolotareff faleceu jovem (com 31 anos): foi atropelado por um trem quando se dirigia a sua casa de campo.

Capítulo 10

Soma de Quadrados

Abordamos aqui a representação de inteiros como soma de dois quadrados, ou seja, dado um inteiro n, estudamos a equação Diofantina não linear

$$a^2 + b^2 = n,$$

tentando determinar quantas soluções tem (se existem), e quais são. Mostramos também que todo inteiro pode ser representado como soma de quatro quadrados.

10.1 Soma de dois quadrados

Começamos identificando quais inteiros podem ser escritos como soma de dois quadrados, e quais deles pode ser escritos como soma de dois quadrados $x^2 + y^2$, com $\mathrm{mdc}\,(x, y) = 1$.

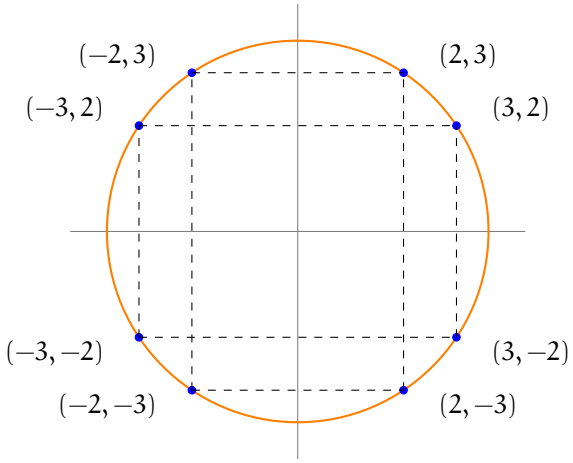
Definição 10.1 (representação de inteiro como soma de quadrados)**.** *Seja n um inteiro positivo. Dizemos que o par de inteiros positivos (x, y) é uma* ***representação*** *de n como soma de dois quadrados se $x^2 + y^2 = n$.*
Se $\mathrm{mdc}\,(x, y) = 1$, dizemos que se trata de uma representação própria *de n.* ◀

Por exemplo, 109 tem representação própria como soma de dois quadrados, já que $109 = 3^2 + 10^2$ e $\mathrm{mdc}\,(3, 10) = 1$.
Já 117 tem representação, mas não própria, porque $117 = 3^2(13)$, e $\mathrm{mdc}\,(6, 9) = 3$. A representação, imprópria, é $117 = 6^2 + 9^2$.
A interpretação geométrica do que significa um inteiro ser soma de dois quadrados é relevante. A expressão $x^2 + y^2 = n$ representa uma circunferência de raio $\sqrt{n}$ centrada na origem. Um par (x, y) que represente n é um ponto nesta circunferência. Contar a quantidade de representações de n como soma de quadrados é o mesmo que contar os pontos inteiros na

circunferência. Por exemplo, se $n = 13$ podemos visualizar a circunferencia com raio $\sqrt{13} \approx 3.605$, e os pontos inteiros na circunferencia são

$$(\pm 2, \pm 3), \quad (\mp 2, \pm 3),$$
$$(\pm 3, \pm 2), \quad (\mp 3, \pm 2),$$

ilustrados na figura a seguir.



Agora começamos demonstrando um Lema.

Lema 10.1. *-1 é resíduo quadrático módulo p se e somente se p é um primo da forma $4k+1$.*

Demonstração. Primeiro, se -1 é quadrado módulo p, então

$$\begin{aligned} 1 &\equiv x^{p-1} && \text{(pequeno teorema de Fermat[1])} \\ &\equiv (x^2)^{\frac{p-1}{2}} \\ &\equiv (-1)^{\frac{p-1}{2}} && \text{(a afirmação vale para todo quadrado...)} \end{aligned}$$

Mas se p fosse $4k+3$, então

$$\begin{aligned} \frac{p-1}{2} &= \frac{4k+3-1}{2} \\ &= 2k+1. \end{aligned}$$

Isso significa que o expoente de -1 é $2k+1$ (ímpar), e teriamos

$$\begin{aligned} (-1)^{\frac{p-1}{2}} &= (-1)^{2k+1} \\ &= -1 \end{aligned}$$

E portanto teríamos chegado a

$$1 \equiv -1 \pmod{p},$$

o que é impossível. Desta forma, necessariamente temos $p = 4k+1$.

Agora, se p é $4k+1$ tal elemento existe e podemos determiná-lo – a congruência, da forma como está escrita, já nos indica que o Teorema de Wilson pode ser usado. Sabemos que $(p-1)! \equiv -1 \pmod{p}$. Então,

$$\begin{aligned} \frac{p+1}{2} \leq x \leq p-1 &\text{ se e somente se} \\ -\frac{p-1}{2} \leq x-p \leq -1. & \qquad \text{(subtraia } p\text{)} \end{aligned}$$

Portanto,

$$\begin{aligned} (p-1)! &\equiv \left(1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}\right) \overbrace{\left(\frac{p+1}{2} \cdot \frac{p+3}{2} \ldots (p-1)\right)}^{\text{cada um} \equiv -1,-2,\ldots,-(p-1)/2 \pmod{p}} \\ &\equiv (-1)^{(p-1)/2}\, 1^2\, 2^2\, 3^2 \cdots \left(\frac{p-1}{2}\right)^2 \\ &\equiv (-1)^{(p-1)/2} \left[\left(\frac{p-1}{2}\right)!\right]^2 \\ &\equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \qquad (p = 4k+1 \;\rightarrow\; (p-1)/2 \text{ é par}) \\ &\equiv -1 \pmod{p}. \qquad \text{(Teorema de Wilson)} \end{aligned}$$

Nas duas últimas linhas está o que de fato interessa: primeiro, $(p-1)/2$ é par, porque p é da forma $4k+1$, e somente por isso a expressão tem sentido neste contexto. Assim,

$$\left[\left(\frac{p-1}{2}\right)!\right]^2$$

deve necessariamente ser congruente a -1 módulo p, pelo Teorema de Wilson. E portanto -1 é quadrado módulo p. □

Neste trecho desenvolvemos $(p-1)!$ até chegar em um quadrado, e em seguida usamos o Teorema de Wilson para mostrar que -1 é quadrado.

A primeira parte da demonstração pode ser refeita usando o teorema de Lagrange[2].

[1] **Teorema 7.4 (de Fermat):** Se p é primo e $p \nmid a$ então

$$a^{p-1} \equiv 1 \pmod{p}.$$

[2] **Teorema 7.18 (de Lagrange):** A ordem de um subgrupo divide a ordem do grupo.

Suponha que $(-1) \equiv x^2 \pmod{p}$. Então

$$\begin{aligned}(-1)(-1) &\equiv +1 \pmod{p}\\ (x^2)(x^2) &\equiv +1 \pmod{p}\\ x^4 &\equiv +1 \pmod{p},\end{aligned}$$

e x tem ordem 4 em $\mathbb{Z}_p$. Isto significa que há um subgrupo de ordem 4. Pelo Teorema de Lagrange, 4 divide $p-1$ (a quantidade de elementos no grupo), e portanto $p = 4k+1$.

Tratamos primeiro de caracterizar quando há representação própria para um inteiro. Depois trataremos do caso impróprio.
A *identidade de Brahmagupta-Fibonacci* (o Teorema 10.1) será útil nas demonstrações dos Teoremas 10.2/10.3 e 10.4

Teorema 10.1 (identidade de Brahmagupta-Fibonacci)**.** *Se* $a, b, c, d \in \mathbb{Z}$*, então*

$$(a^2+b^2)(c^2+d^2) = (ac \mp bd)^2 + (ad \pm bc)^2.$$

Teorema 10.2. *Um inteiro positivo* n *tem representação própria se e somente se não tem fatores da forma* $4k+3$*.*

O Teorema 10.2 pode ser também redigido de forma ligeiramente diferente:

Teorema 10.3. *Seja um inteiro positivo* $n = b^2c$*, onde* c *é livre de quadrados. Então* n *é soma de dois quadrados se e somente se não existe primo* $p = 4k+3$ *tal que* $p \mid c$*.*

Demonstração. ($\Rightarrow$) Seja $p = 4k+3$ um fator de $n = x^2+y^2$. Então, suponha que $y \not\equiv 0 \pmod{p}$ (ou seja, $p \nmid y$).

$$\begin{aligned}x^2 + y^2 &\equiv 0 \pmod{p}\\ x^2 &\equiv -y^2 \pmod{p}\\ xy^{-1}(^2) &\equiv -1 \pmod{p}\end{aligned}$$

Mas -1 não pode ser quadrado módulo p, porque p é da forma $4k+3$. Então $y \equiv 0 \pmod{p}$. De maneira simétrica, $x \equiv 0 \pmod{p}$, e $p \mid x$, $p \mid y$. Mas como

$$n = x^2 + y^2$$

então $p^2 \mid n$, e

$$\frac{n}{p^2} = \left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2,$$

e temos que n/p^2 tem representação como soma de dois quadrados. Se continuarmos, dividiremos n por uma porência *par*. Desta forma, p não pode dividir n um número ímpar de vezes (ou, usando a segunda forma do enunciado do Teorema, p não pode dividir o fator c livre de quadrados).

($\Leftarrow$) É fácil verificar que se a e b são cada um soma de dois quadrados, então ab também é, pela identidade de Brahmagupta-Fibonacci:

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

É simples agora verificar por indução no número de fatores de n que se n não tem potências ímpares de primos $4k + 3$ na fatoração, então n é soma de quadrados. □

Teorema 10.4. *Um inteiro positivo n é representável como soma de dois quadrados se e somente se sua fatoração em primos não contém potências ímpares de primos da forma $4k + 3$.*

Exemplo 10.1. *O número $275 = (11)5^2$ contém uma potência ímpar de 11, que é da forma $4k + 3$, por isso não pode ser representado como soma de dois quadrados.*

O número $45 = (5)3^2$ rem uma potência par de 3, que é obviamente da forma $4k + 3$, e é representável por dois quadrados:

$$\begin{aligned} 45 &= 36 + 9 \\ &= 6^2 + 3^2. \end{aligned}$$

A representação é, no entanto, imprópria, já que $\mathrm{mdc}\,(6, 3) = 3$. ◀

Demonstração. ($\Rightarrow$) Seja p um primo da forma $4k + 3$, e suponha que $p \mid n$, e que $2r + 1$ é a ordem de p na fatoração de n. Suponha também que $n = x^2 + y^2$, com $x, y \in \mathbb{N}^*$, com $\mathrm{mdc}\,(x, y) = d$. Como $p \mid n$, então alguma potência de p divide d.

Então dividimos x e y por d e escrevemos

$$\begin{aligned} x/d = x' \quad &\Rightarrow \quad x = dx' \\ y/d = y' \quad &\Rightarrow \quad y = dy' \end{aligned}$$

Agora temos $\mathrm{mdc}\,(x', y') = 1$. Seja

$$\begin{aligned} m &= (x')^2 + (y')^2 \\ &= \left(\frac{x}{d}\right)^2 + \left(\frac{y}{d}\right)^2. \end{aligned}$$

Assim, m é um inteiro com representação própria. Mas

$$\begin{aligned} p^{2r+1} &\mid n \\ p^{2r+1} &\mid x^2 + y^2 \\ p^{2r+1-2j} &\mid (x')^2 + (y')^2 \qquad \text{(divida por } d^2\text{)} \end{aligned}$$

Isto contradiz o Teorema 10.2, porque m será um inteiro com representação própria, e com $p = 4k + 3$ em sua fatoração.

($\Leftarrow$) Agora mostramos que, se na fatoração de um inteiro n os primos da forma $4k+3$ só aparecem com expoentes pares, então n tem representação como soma de quadrados. Assim, presumimos que

$$n = ab^2,$$

onde a é livre de quadrados e não tem fatores primos da forma $4k + 3$. Nos basta provar que a é representável, porque b^2 evidentemente é, e o produto de inteiros representáveis é, também, representável:

$$(a^2 + b^2)(\alpha^2 + \beta^2) = (a\alpha + b\beta)^2 + (a\beta - b\alpha)^2.$$

Agora, a é produto de primos da forma $4k+1$. Precisamos somente mostrar que todo primo desta forma é representável. Mas pelo Lema 10.1[3], a congruência $x^2 \equiv -1 \pmod{p}$ tem solução, e a é representável como soma de quadrados. Mas se a é representável, n também é. □

Finalmente, retomamos a interpretação geométrica do início do Capítulo: se iniciarmos da origem e abrirmos continuamente uma circunferência, aumentando seu raio, em determinados momentos ela passará por exatamente oito pontos inteiros, (x, y) com todas as possibilidades de sinal. Se r é o raio, os momentos em que a circunferência tocará pontos inteiros são:

i) quando a fatoração de r não tem qualquer primo da forma $4k + 3$, e neste caso $\mathrm{mdc}\,(x, y) = 1$;

ii) quando a fatoração de r tem somente potências pares de primos $4k+3$, e neste caso $\mathrm{mdc}\,(x, y) > 1$.

[3] **Lema 10.1:** -1 é resíduo quadrático módulo p se e somente se p é um primo da forma $4k + 1$.

10.2 Soma de quatro quadrados

Lagrange demonstrou em 1770 que sempre é possível representar um inteiro positivo como soma de quatro quadrados[4] (e portanto como soma de k quadrados, para qualquer $k \geq 4$).

Teorema 10.5. *Seja p primo. Então existem x, y, z inteiros, pelo menos um deles diferente de zero, tais que*

$$x^2 + y^2 + z^2 \equiv 0 \pmod{p}.$$

Demonstração. Trataremos separadamente três casos: $p = 2$, $p = 4k + 1$, e $p = 4k + 3$.
Para $p = 2$, temos $x = y = 1$ como solução (com $z = 0$).
Para $p = 4k + 1$, escolhemos $y = 1$, $z = 0$, e obtemos x resolvendo a congruência $x^2 \equiv -1 \pmod{p}$.
Para $p = 4k + 3$, determinamos $z = 1$, e resolvemos a congruência: $x^2 + y^2 + 1 \equiv 0 \pmod{p}$. Seja d o menor número positivo que não é resíduo

[4] A demonstração de Lagrange foi feita usando propriedades de formas quadráticas.

Lagrange, Joseph-Louis. **Ouvres de Lagarange**. Edição: M. J.-A Serret. [*S. l.*]: Gauthier Villars, 1867. v. 3.

O artigo, "Démonstration d'un théorème d'arithmétique" está na página 189. Esta é uma reprodução em uma coletânea. O original é

Lagrange, Joseph-Louis. Démonstration d'un théorème d'arithmétique. **Nouveaux mémoires de l'Académie royale des sciences et belles-lettres de Berlin**, p. 122–133, 1770.

No artigo, Lagrange menciona que

> *É um teorema conhecido há bastante tempo que qualquer número inteiro não quadrado sempre pode ser decomposto em dois, três ou quatro quadrados inteiros; mas ninguém, que eu saiba, proveu uma demonstração. O Sr. Bachet de Méziriac foi o primeiro a mencionar este Teorema; parece que ele foi motivado pela questão 31 do IV Livro de Diofante, onde o Teorema do qual estamos falando é de alguma forma tacitamente suposto; mas o Sr. Bachet contentou-se em verificar a verdade deste Teorema por indução, examinando sucessivamente todos os números inteiros de 1 a 325; e quanto à demonstração geral, admite que ainda não a conseguiu.*

No original,

> *C'est un Théorème connu depuis longtemps que tout nombre entier non carré peut toujours se décomposer en deux, ou trois, ou quatre carrés entiers; mais personne, que je sache, n'en a encore donné la démonstration. M. Bachet de Méziriac est le premier qui ait fait mention de ce Théorème; il paraît qu'il y a été conduit par la question 31^e du IV^e Livre de Diophante, où le Théorème dont nous parlons est en quelque sorte tacitement supposé; mais M. Bachet s'est contenté de s'assurer de la vérité de ce Théorème par induction, en examinant successivement tous les nombres entiers depuis 1 jusqu'à 325; et quant à la démonstration générale, il avoue qu'il n'avait pas encore pu y parvenir.*

O que Lagrange chama de "indução" não é a técnica que conhecemos – ele fala de verificar vários casos particulares, e a partir disso supor que o caso geral vale.
Lagrange também menciona brevemente uma tentativa de Euler de demonstrar o teorema.

quadrático módulo p. Então temos

$$\left(\frac{-d}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{d}{p}\right) = (-1)(-1) = +1.$$

Portanto $-d$ é resíduo quadrático modulo p, e $d \geq 2$, porque d não é resíduo quadrático. Escolhemos y tal que $y^2 \equiv -d \pmod{p}$.
Sabemos que $d \geq 2$, e também que d é o menor resíduo não-quadrático módulo p, logo $d-1$ deve ser resíduo quadrático módulo p. e x Assim, escolhemos x tal que $x^2 \equiv d-1 \pmod{p}$.
Temos portanto

$$\begin{aligned} x^2 + y^2 + z^2 &\equiv (d-1) + (-d) + 1 && \pmod{p} \\ &\equiv 0 && \pmod{p}. \end{aligned}$$

□

Da demonstração extraímos o Corolário 10.1.

Corolário 10.1. *Para todo p primo, existem u, v, tais que $u^2 + v^2 \equiv -1 \pmod{p}$.*

O Lema 10.2, de fácil verificação, será útil na demonstração do Teorema dos quatro quadrados.

Lema 10.2. *Sejam α, β inteiros Gaussianos tais que $\alpha \equiv \beta \pmod{p}$. Então $\alpha\overline{\alpha} \equiv \beta\overline{\beta} \pmod{p}$.*

Teorema 10.6 (de Lagrange)**.** *Todo inteiro é representável como soma de quatro quadrados*[5]*.*

Demonstração. Como o produto de números representáveis por quatro quadrados é representável, só precisamos mostrar que primos são representáveis.
Quando $p = 2$ e $p = 3$ o Teorema é trivialmente válido. Suponha, portanto, que $p > 3$.
Sejam u, v tais que $u^2 + v^2 \equiv -1 \pmod{p}$ (cuja existência é garantida pelo Corolário 10.1), e $k = \lfloor\sqrt{p}\rfloor$.
O conjunto de inteiros Gaussianos

$$\{(a + bi) - (c + di)(u + vi) \ : \ a, b, c, d \in [0, k] \cap \mathbb{Z}\}$$

[5] O enunciado, como originalmente declarado por Lagrange, é

> *Todo número inteiro não quadrado sempre pode ser decomposto em dois, tres, ou quatro quadrados inteiros.*

No original,

> *Tout nombre entier non carré peut toujours se décomposer en deux, ou trois, ou quatre carrés entiers.*

tem $(k+1)^4$ elementos. Como $(k+1)^4 > p^2$, pelo princípio da casa dos pombos deve haver pelo menos dois destes números que são congruentes módulo p. Sejam eles $(a_1 + b_1 i) - (c_1 + d_1 i)(u + vi)$ e $(a_2 + b_2 i) - (c_2 + d_2 i)(u + vi)$. Agora, definimos

$$\begin{aligned} A &= a_1 - a_2 \\ B &= b_1 - b_2 \\ C &= c_1 - c_2 \\ D &= d_1 - d_2. \end{aligned}$$

Sabemos que

$$|A|, |B|, |C|, |D| \leq k,$$

porque $a, b, c, d \leq k$. Além disso, nem todos são zero.

Tomamos A, B, C, D e escrevemos

$$\begin{aligned} A + Bi &\equiv (C + Di)(u + vi) \pmod{p} \\ (A + Bi)(A - Bi) &\equiv (C + Di)(C - Di)(u + vi)(u - vi) \pmod{p} \qquad \text{(Lema 10.2)} \\ A^2 + B^2 &\equiv (C^2 + D^2)(u^2 + v^2) \pmod{p} \\ A^2 + B^2 &\equiv -C^2 - D^2 \pmod{p} \qquad (u^2 + v^2 \equiv -1) \\ A^2 + B^2 + C^2 + D^2 &\equiv 0 \pmod{p}. \end{aligned}$$

Então, $p|Z = A^2 + B^2 + C^2 + D^2$. Seja

$$Z \leq 4k^2 \leq 4p$$

Necessariamente, $Z = tp$, onde t pode ser 1, 2 ou 3.

Se $t = 1$,

$$p = A^2 + B^2 + C^2 + D^2,$$

como no enunciado.

Quando $t = 2$,

$$2p = A^2 + B^2 + C^2 + D^2.$$

Nesta situação há três possibilidades para a paridade dos números A, B, C, D: todos pares; todos ímpares; ou dois pares e dois ímpares. De qualquer forma, presumiremos, sem perda de generalidade, que A e B tem a mesma paridade; e que C e D tem a mesma paridade (não necessariamente a mesma que A e B). Assim, temos

$$\begin{aligned} A \pm B &\text{ é par} \\ C \pm D &\text{ é par} \end{aligned}$$

Então

$$\begin{aligned} 2p &= A^2 + B^2 + C^2 + D^2 \\ p &= \frac{A^2}{2} + \frac{B^2}{2} + \frac{C^2}{2} + \frac{D^2}{2} \\ &= \left(\frac{A+B}{2}\right)^2 + \left(\frac{A-B}{2}\right)^2 + \left(\frac{C+D}{2}\right)^2 + \left(\frac{C-D}{2}\right)^2. \end{aligned}$$

Como as somas nos numeradores são pares, as frações acima são todas inteiras, e p é representável como soma de quatro quadrados.

Finalmente, quando $t = 3$,

$$3p = A^2 + B^2 + C^2 + D^2.$$

Para qualquer inteiro k, temos que $k^2 \equiv 0 \pmod 3$ ou $k^2 \equiv 1 \pmod 3$, porque quadrados não podem deixar resto 2 quando divididos por 3. Trataremos agora os dois casos:

i) todos os quadrados na fórmula acima são divisíveis por 3;

ii) três deles deixam resto um, e o outro é divisível por 3: $a^2, b^2, c^2 \equiv 1 \pmod 3$, mas $d^2 \equiv 0 \pmod 3$.

No caso (i), como a^2, b^2, c^2, d^2 são quadrados divisíveis por 3, são também divisíveis por nove.

$$\begin{aligned} 3p &= A^2 + B^2 + C^2 + D^2 \\ 3p &= 9A' + 9B' + 9C' + 9D' \\ p &= \frac{9A'}{3} + \frac{9B'}{3} + \frac{9C'}{3} + \frac{9D'}{3} \\ p &= 3A' + 3B' + 3C' + 3D' \\ p &= 3w, \end{aligned}$$

mas p é primo, e $p > 3$, logo não pode ser múltiplo de 3.

Observamos o caso (ii). Suponha, sem perda de generalidade, que $A^2, B^2, C^2 \equiv 1 \pmod 3$, e $D^2 \equiv 0 \pmod 3$. Então

$$\begin{aligned} A &\equiv \pm 1 \pmod 3 \\ D &\equiv 0 \pmod 3. \end{aligned}$$

No entanto, podemos trocar A por $-A$ se necessário (porque será elevado

ao quadrado), e dizer que $A \equiv +1 \pmod 3$.

$$\begin{aligned} n_1 &= A + B + C \\ n_2 &= A - B + D \\ n_3 &= -A + C + D \\ n_4 &= B - C + D \end{aligned}$$

$$\begin{aligned} n_1^2 + n_2^2 + n_3^2 + n_4^2 &= (A + B + C)^2 + (A - B + D)^2 + (-A + C + D)^2 + (B - C + D)^2 \\ &= 3(A^2 + B^2 + C^2 + D^2) \\ &= 9p \end{aligned}$$

Logo,

$$p = \left(\frac{n_1}{3}\right)^2 + \left(\frac{n_2}{3}\right)^2 + \left(\frac{n_3}{3}\right)^2 + \left(\frac{n_4}{3}\right)^2,$$

e completamos a demonstração. □

10.3 Soma de três quadrados

O problema da representação de inteiros como soma de três quadrados é bem mais difícil, em parte porque para três quadrados não podemos contar com uma regra de composição que vale para dois e para quatro quadrados: enquanto 3 e 5 são representáveis como soma de três quadrados ($3 = 1 + 1 + 1$; $5 = 4 + 1 + 0$), 15 não é.

Enunciamos agora um Teorema de Gauss-Legendre[6] que dá as condições para que um inteiro seja representável como soma de três quadrados, mas apresentamos a demonstração de apeans uma direção do "se e somente se".

Teorema 10.7 (de Gauss-Legendre)**.** *Um inteiro positivo é representável como soma de três quadrados se e somente se não é da forma* $4^m(8k+7)$.

Demonstração. (*apenas o "somente se")* Todo quadrado é congruente a $0, 1$ ou 4 módulo 8.
Assim, a soma de três quadrados só pode ser congruente a $0, 1, 2, 3, 4, 5$ ou 6 módulo oito (ou seja, qualquer dos possíveis restos, exceto sete). Nenhum número da forma $8k+7$ (ou seja, nenhum número $x \equiv 7 \pmod 8$), portanto, é representável.
Se $4 \mid n$ e n é soma de três quadrados, $n = x^2 + y^2 + z^2$, então x, y, z devem ser pares de forma que se possa dividir seus quadrados por 4. Mas isso significa que $n/4$ também deveria ser soma de quadrados. Logo, se

[6] Legendre. Não Lagrange, do teorema dos quatro quadrados!
Legendre e Gauss disputaram a autoria de diversos teoremas, inclusive este. Em particular, a demonstração de Legendre para este Teorema presumia, como se fosse evidente, a existência de infinitos primos em qualquer progressão aritmética; mas isto só foi estabelecido posteriormente por Dirichlet, usando métodos de Análise.
A demonstração de Legendre para o Teorema de três quadrados está aqui:

> **Legendre**, Adrien-Marie. **Essai sur la théorie des nombres**. [*S. l.*]: Paris, Duprat, 1798. Disponível em `https://archive.org/details/essaisurlathor00lege`.

Artigo 331, na página 398:

> **TEOREMA XXI.** *Todo número ímpar, exceto somente os números* $8n+7$*, é a soma de três quadrados.*

O original:

> **THÉORÊME XXI.** *Tout nombre impair , excepté seulement les nombres* $8n+7$*, est la somme de trois quarrés.*

A demonstração de Legendre segue como consequência da discussão anterior no mesmo texto (*"Esta proposição é agora um corolário muito simples da teoria anterior" – "Cette proposition est maintenant un corollaire très-simple de la théorie précédente"*).
A forma como enunciamos o teorema é diferente – foi Cauchy, em 1813, que provou que o teorema de Legendre é equivalente ao anunciado que damos no texto.
Gauss enuncia e demonstra o mesmo teorema como aplicação da teoria de formas quadráticas, nos artigos 288 e 289 do *Disquisitiones*. No artigo 288, em particular, lemos

> **PROBLEMA.** *Dado um número positivo* M*, para encontrar as condições sob as quais há formas binárias primitivas negativas de determinante* $-M$ *que são resíduos quadráticos de* M*, ou em outras palavras, para os quais* 1 *é número característico.*

No original:

> **PROBLEMA.** *Designante* M *numerum positivum, inveniere conditiones sub quibus formae binariae primitivae negativae determinantis* $-M$ *dari possint, quae sint resitua quadratica ipsius* M *sive pro quibus* 1 *sit numeris characteristicus.*

O artigo seguinte (289) determina que M deve ser divisível por 4 ou da forma $8n+7$.

n é soma de quadrados, não pode ser quatro vezes um número que não é representável. □

Uma interessante consequência do Teorema dos três quadrados é estabelecida pelo Teorema[7] 10.8

Teorema 10.8. *Todo inteiro positivo pode ser escrito como soma de três números triangulares*

Demonstração. Considere a equação

$$8n + 3 = x^2 + y^2 + z^2$$

Módulo 8, é necessário que x, y, z sejam ímpares.
Sejam a, b e c, ímpares:

$$x = 2a + 1$$
$$y = 2b + 1$$
$$z = 2c + 1$$

[7] Gauss demonstrou este teorema no *Disquisitiones, usando o mesmo argumento.*

Gauss, Johann Carl Friedrich. **Disquisitiones Arithmeticae**. [*S. l.*], 1801.

Artigo 293:

> *O argumento anterior também provê uma demonstração daquele famoso Teorema: todo inteiro positivo pode ser decomposto em três números triangulares. Foi descoberto por Fermat mas até agora não havia demonstração rigorosa para ele. É manifesto que qualquer decomposição do número M em três números triangulares*
>
> $$\frac{1}{2}x(x+1) + \frac{1}{2}y(y+1) + \frac{1}{2}z(z+1)$$
>
> *produzirá uma decomposiçào do número $8M + 3$ em três quadrados ímpares*
>
> $$(2x+1)^2 + (2y+1)^2 + (2z+1)^2$$
>
> *e vice-versa.*

O original:

> *Disquisitiones praecedentes etiam suppeditant demonstrationem theorematis famosi, omnem numerum integrum positivum in tres numeros trigonales discrepi posse, quod a Fermatio olim inventum est, sed cuius demonstratio rigorosa hactenus desiderabatur. Manifestum est, quamvis discreptionem numeri M in trigonales*
>
> $$\frac{1}{2}x(x+1) + \frac{1}{2}y(y+1) + \frac{1}{2}z(z+1)$$
>
> *producere discreptionem numeri $8M + 3$ in terna quadrata imparia*
>
> $$(2x+1)^2 + (2y+1)^2 + (2z+1)^2$$
>
> *et vice versa.*

Em seu diário, Gauss escreveu "*EYPHKA*! $\text{num} = \Delta + \Delta + \Delta$" – e o Teorema é muitas vezes chamado de "Teorema Eureka", de Gauss.

Substitua na primeira equação:

$$
\begin{aligned}
8n+3 &= x^2+y^2+z^2 \\
8n+3 &= (2a+1)^2+(2b+1)^2+(2c+1)^2 \\
n &= \frac{(2a+1)^2+(2b+1)^2+(2c+1)^2-3}{8} \\
n &= \frac{4a^2+4a+1+4b^2+4b+1+4c^2+4c+1-3}{8} \\
n &= \frac{4a^2+4a+4b^2+4b+4c^2+4c}{8} \\
n &= \frac{4a(a+1)+4b(b+1)+4c(c+1)}{8} \\
n &= \frac{a(a+1)}{2}+\frac{b(b+1)}{2}+\frac{c(c+1)}{2}
\end{aligned}
$$

Pela demonstração dada no Exemplo[8] 2.4, n é a soma de três numeros triangulares. □

10.4 Quantidade de representações

Tendo estabelecido quando existe representação para um inteiro como soma de dois quadrados, tratamos agora de calcular a quantidade de representações de cada inteiro.

Definição 10.2. $R(n)$ *é a quantidade de representações de* n*;*
$r(n)$ *é a quantidade de representações próprias de* n*;*
$P(n)$ *é a quantidade de representações próprias de* n *com* $x>0$*;*
$N(n)$ *é a quantidade de soluções da congruência* $a^2 \equiv -1 \pmod{n}$*.* ◀

Teorema 10.9. $\forall n>0,\ \ r(n)=4N(n)$.

Demonstração. Provamos o caso $n=1$ separadamente. Todo número é congruente a zero módulo um, já que a divisão por um nunca deixa resto. Assim, a equação $u^2 \equiv -1 \pmod{1}$ tem uma única solução (a única classe de congruências módulo um, representada pelo zero). Temos $N(1)=1$, e o número de representações de um é, portanto, $4N(1)=4$. De fato,

$$
\begin{aligned}
1 &= (+1)^2+0^2 \\
&= (-1)^2+0^2 \\
&= \quad 0^2 \ +(+1)^2 \\
&= \quad 0^2 \ +(-1)^2
\end{aligned}
$$

[8] Exemplo de demonstração por indução. Ali fica estabelecido que o k-ésimo número triangular é $T_k = \frac{k(k+1)}{2}$.

Estas representações são próprias, porque $\mathrm{mdc}\,(0, \pm 1) = 1$.
Quando $n > 1$ e $n = x^2 + y^2$, vemos que necessariamente tanto x como y devem ser diferentes de zero, porque tratamos de representações próprias, e necessitamos que $\mathrm{mdc}\,(x, y) = 1$.
Como x e y são diferentes de zero, o número total de representações é igual a quatro vezes o número de representações positivas (para contabilizarmos as quatro possibilidades de sinais para x e y). Só precisamos agora mostrar que a quantidade de soluções de $u^2 \equiv -1 \pmod{n}$ é igual à quantidade de representações positivas de n.
Suponha que $n = x^2 + y^2$, com $x, y > 0$ e $\mathrm{mdc}\,(x, y) = 1$. Então a equação $y \equiv ux \pmod{n}$ tem uma única solução[9]. Podemos substituir y por ux, como a seguir.

$$\begin{aligned} x^2 + y^2 &\equiv x^2 + (ux)^2 && \pmod{n} \\ &\equiv x^2(u+1)^2 && \pmod{n} \\ &\equiv 0 && \pmod{n} \end{aligned}$$

Mas como $x^2 > 0$, é necessário que $(u+1)^2 \equiv 0 \pmod{n}$, e $u^2 \equiv -1 \pmod{n}$. Agora, para cada u com $u^2 \equiv -1 \pmod{n}$, se tomarmos $y \equiv ux \pmod{n}$, teremos

$$\begin{aligned} y &\equiv ux && \pmod{n} \\ y^2 &\equiv u^2x^2 && \pmod{n} \\ y^2 &\equiv -x^2 && \pmod{n} \\ x^2 + y^2 &\equiv 0 && \pmod{n} \end{aligned}$$

E temos exatamente uma representação positiva para u. □

Teorema 10.10. *Para todo inteiro $n > 0$,*

$$R(n) = \sum_{d^2 \mid n} r\left(\frac{n}{d^2}\right)$$

Demonstração. Suponha que n é representado por x e y, e $\mathrm{mdc}\,(x, y) = d$. Dividimos a equação $x^2 + y^2 = n$ por d^2, e obtemos

$$\left(\frac{x}{d}\right)^2 + \left(\frac{y}{d}\right)^2 = \frac{n}{d^2}.$$

Isto nos dá uma representação própria de n/d^2, porque $\mathrm{mdc}\,(x/d.\, y/d) = 1$.

[9] Porque $y \equiv ux \pmod{n}$ é o mesmo que $y - ux = kn$, e $\mathrm{mdc}\,(x, y) = 1 \mid n$.

Agora suponha que u, w sejam representação própria de n/d^2, então

$$(ud)^2 + (wd)^2 = n$$

é representação de n, com $\mathrm{mdc}\,(ud, wd) = d$.
Mostramos que há uma correspondência um-para-um entre as representações de n e as representações próprias de n/d^2, como no enunciado. □

Lema 10.3. $N(n) = 2^{s+1}$, *onde* s *é a quantidade de primos distintos da forma* $4k+1$ *que dividem* n.

Demonstração. A fatoração de n pode ser escrita como

$$n = 2^h \left(\prod_p p^i\right)\left(\prod_q q^j\right),$$

onde os primos p são da forma $4k+1$ e os primos q são da forma $4k+3$. Como $N(n)$ é o número de soluções de uma congruência polinomial, então pelo Teorema[10] 6.21,

$$N(n) = N\left(2^h\right)\prod_i N\left(p^i\right)\prod_j N\left(q^j\right).$$

Analisamos as três partes do lado direito, separadamente.
Para ps primos da forma 2^h,

$$\begin{aligned} N(2^1) &= N(2) = 1, \\ N(2^2) &= N(4) = 0, \\ N(2^h) &= 0, \quad h > 2 \end{aligned}$$

ou seja, somente $a^2 = -1 \pmod 2$ tem uma solução, e $a^2 = -1 \pmod{2^h}$ não tem solução quando $h > 1$.
Para os primos da forma $4k+3$, pelo Lema[11] 10.1,

$$N(q^j) = 0, \;\; j > 0$$

Mas para os da forma $4k+1$,

$$N(p) = 2$$

[10] **Teorema 6.21:** Seja $f(x)$ um polinômio com coeficientes inteiros, e m um inteiro positivo. Denote por $N(m)$ a quantidade de soluções da congruência $f(x) \equiv 0 \pmod m$. Então, se $m = m_1 m_2$, com m_1 e m_2 co-primos, $N(m) = N(m_1)N(m_2)$.
[11] **Lema 10.1:** -1 é resíduo quadrático módulo p se e somente se p é um primo da forma $4k+1$.

Pelo Lema de Hensel[12],

$$N(p^i) = 2, \quad i > 0$$

Assim,

$$N(n) = (2)(2^s)(1) = 2^{s+1}$$

onde s é a quantidade de primos distintos da forma $4k+1$. □

Teorema 10.11. *Seja n um número tendo representação própria como soma de dois quadrados, e s a quantidade de primos da forma $4k+1$ que dividem n. Então $r(n) = 2^{s+2}$.*

Demonstração. Pelo Lema 10.3 e o Teorema 10.9,

$$r(n) = 4N(n) = (2^2)(2^s) = 2^{s+1}.$$ □

Teorema 10.12. *Seja n um número representável como soma de dois quadrados:*

$$n = 2^h \prod_p p^i \prod_q q^j,$$

onde os primos p são da foram $4k+1$ e os primos q são da forma $4k+3$. Então $R(n) = 4\prod_p (i+1)$.

A fórmula determina o produto do expoente de cada primo p.

Exemplo 10.2. *Seja $n = 13$. O número é apenas um primo da forma $4k+1$. Assim,*

$$13 = (2^0)(13^1)(1).$$

O expoente é 1, portanto a quantidade de representações é

$$R(13) = 4(1+1) = 8,$$

que coincide com o que verificamos no início do Capítulo.
Já 25 é $25 = (2^0)(5^2)(1)$, portanto

$$R(25) = 4(1+2) = 12.$$

E realmente, as representações de 25 são dadas pelos pares

$$(0, \pm 5), (5, \pm 0)$$
$$(\pm 3, \pm 4)(\mp 3, \pm 4)$$
$$(\pm 4, \pm 3)(\mp 4, \pm 3),$$

doze casos.

[12] **Lema 6.7 (de Hensel):** Seja $f(x)$ um polinômio com coeficientes inteiros. Se $x \in \mathbb{Z}$, $f(x) \equiv 0 \pmod{p^b}$ e $f'(x) \not\equiv 0 \pmod{p}$, então existe um único t inteiro positivo tal que $f(x + tp^b) \equiv 0 \pmod{p^{b+1}}$.

Agora, se $n = 45 = 2^0 3^2 \cdot 5$*, temos* 3^2*, um primo* $4k+3$ *com expoente dois, e* 5*, um primo* $4k+1$ *com expoente* 1*. Ignoramos o* 3^2 *e calculamos*

$$R(45) = 4(1+1) = 8.$$

As representações de 45 *são dadas pelos pares*

$$(\pm 3, \pm 6)(\mp 3, \pm 6)$$
$$(\pm 6, \pm 3)(\mp 6, \pm 3),$$

oito casos.
Analisamos um último caso: $n = 650$*. Agora* $n = (2^1)(5^2)(13^1)$*. Novamente ignoramos os fatores que não são* $4k+1$ *(neste caso o* 2*), e computamos*

$$R(650) = 4(2+1)(1+1) = 24.$$

As representações de 650 *como soma de quadrados são dadas pelos pares*

$$(\pm 5, \pm 25), (\mp 5, \pm 25),$$
$$(\pm 25, \pm 5), (\mp 25, \pm 5),$$
$$(\pm 11, \pm 23), (\mp 11, \pm 23),$$
$$(\pm 23, \pm 11), (\mp 23, \pm 11),$$
$$(\pm 17, \pm 19), (\mp 17, \pm 19),$$
$$(\pm 19, \pm 17), (\mp 19, \pm 17),$$

vinte e quatro casos. ◀

Demonstração. A fatoração do número n é

$$n = (2^h)\left(\prod p^i\right)\left(\prod q^j\right),$$

onde $\prod p^i$ é o produto de primos da forma $4k+1$, cada primo com seu expoente i, e $\prod q^j$ é produto de primos da forma $4k+3$, cada um com seu expoente j.

$$\sum_{d^2|n} N\left(\frac{n}{d^2}\right) = \left(\underbrace{\sum_{d^2|2^h} N\left(\frac{2^h}{d^2}\right)}_{(i)}\right) \prod_p \left(\underbrace{\sum_{d^2|p^i} N\left(\frac{p^i}{d^2}\right)}_{(ii)}\right) \prod_q \left(\underbrace{\sum_{d^2|q^j} N\left(\frac{q^j}{d^2}\right)}_{(iii)}\right)$$

(i) $N(2^1) = 2$, e $N(2^t) = 0$ para $t > 2$, conforme passo na demonstração do Lema[13] 10.3. Então, se h é par, somente um termo no somatório

[13] **Lema 10.3:** $N(n) = 2^{s+1}$, onde s é a quantidade de primos distintos da forma $4k+1$ que

será igual a um, $d = 2^{h/2}$, porque $d^2 = 2^h$ e $2^h/d^2 = 1$. Os outros termos serão zero. Se h é ímpar, o termo com $d = 2^{(h-1)/2}$ será um, e os outros zero. De qualquer forma, o valor do somatório será 1;

(ii) Se i é par, $N(p^i/d^2) = 2$, para $(p/2)$ valores: $d \in \{1, p, p^2, \cdots p^{i/2-1}\}$. Se i é ímpar, $N(p^i/d^2) = 2$ para $d \in \{1, p, p^2, \cdots p^{(i-1)/2}\}$ – ou seja, o somatório resulta em $i+1$ de qualquer forma.

(iii) Quando j é par, q divide todos os q^j/d^2, e este termo desaparece. Quando j é ímpar, então o termo com $d = q^{(i/2)}$ é um, e os outros somem,e o produtório será um.

Pelo Teorema[14] 10.9, $R(n) = 4N(n) = 4(1)\prod_p(i+1)(1) = 4\prod_p(i+1)$. □

Exercícios

Ex. 282 — Prove que se p é um primo da forma $4k+1$ então p pode ser representado *unicamente* (a não ser por ordem e sinal) como soma de dois quadrados.

Ex. 283 — Quantas triplas existem de inteiros consecutivos, todos os três representáveis como soma de dois quadrados?

Ex. 284 — Prove que, se $n > 0$, então

$$R(n) = 4 \sum_{\substack{d|n \\ \text{dímpar}}} \left(\frac{-1}{d}\right).$$

Ex. 285 — Sem usar a fatoração dos números nos argumentos, prove que se m e n são representáveis como soma de dois quadrados ($m = a^2 + b^2$, $n = c^2 + d^2$), então mn também é soma de dois quadrados.

Ex. 286 — Prove que $m = a^2 - b^2$ se e somente se m é fatorável em dois pares ou dois ímpares.

Ex. 287 — Prove que se n é representável como soma de dois quadrados de racionais ($n = (a/b)^2 + (c/d)^2$), então n também é representável como soma de dois quadrados de inteiros.

Ex. 288 — Como corolário do Exercício 287, mostre que um racional m/n é soma de quadrados de dois racionais se e somente se mn é soma de dois quadrados de inteiros.

---

dividem n.

[14] **Teorema 10.9:** $\forall n > 0,\ \ r(n) = 4N(n)$.

Ex. 289 — Releia o último parágrafo da Seção 10.1 (soma de dois quadrados), sobre a interpretação geométrica, e observe geometricamente o que significa o caso (ii).

Ex. 290 — Prove que se p é primo e

$$\left(\frac{-1}{p}\right) = -1$$

então p é norma de um inteiro gaussiano irredutível.

Ex. 291 — Verifique o Corolário 10.1 e o Lema 10.2.

Ex. 292 — Prove que, *como consequência direta do Teorema de Gauss-Legendre*, todo inteiro é a soma de quatro quadrados (não use o Teorema 10.5 nem o caminho usado na demonstração de Lagrange. Só é necessário mostrar que todo inteiro *da forma* $4^a(8k+7)$ é representável).

Ex. 293 — Prove o Teorema dos quatro quadrados de Lagrange, desta vez usando o seguinte argumento. Primeiro, defina

$$A = \begin{pmatrix} p & 0 & r & s \\ 0 & p & s & -r \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

e considere o reticulado gerado por A em $\mathbb{R}^4$. Considere a bola em $\mathbb{R}^4$ com pontos $x = (x_1, x_2, x_3, x_4)$ tais que $x_1^2 + x_2^2 + x_3^3 + x_4^4 < 2p$. Observe o volume da bola, e argumente que existe algum ponto *do reticulado* tal que $x_1^2 + x_2^2 + x_3^3 + x_4^4 = p$.

Ex. 294 — As funções aritméticas definidas neste Capítulo são aditivas? Multiplicativas?

Ex. 295 — Seja $r_k(n)$ a quantidade de representações de n como soma de k quadrados. r_k é aditiva? Multiplicativa?

Parte II

Capítulo 11

Formas Quadráticas

O Capítulo 10 trata da representações de inteiros como soma de dois, três ou quatro quadrados. Passamos agora à generalização dessa idéia para a representação de inteiros por *formas quadráticas*[1], como por exemplo $ax^2 + bxy + cy^2$.
Uma forma quadrática é uma soma da forma

$$f(x_1, x_2, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j,$$

e uma forma quadrática é binária quando é definida para duas variáveis, e escrevemos

$$f(x, y) = ax^2 + bxy + cy^2.$$

11.1 Formas Bilineares e Quadráticas

Definiremos formas quadráticas a partir de formas bilineares.

Definição 11.1 (forma bilinear)**.** *Uma **forma bilinear** em um espaço vetorial V de dimensão finita sobre um corpo K é uma função $f : V \times V \to K$ que é linear em cada um deseus argumentos, ou seja, para todos $u, v, w \in V$ e*

[1] Na verdade os três capítulos, Formas Quadráticas, Formas Modulares e Corpos Quadráticos formam um todo coeso. A apresentação dada aqui para formas quadráticas não é a mais abstrata e moderna, hoje usual na Álgebra/Teoria Algébrica de Números; ela parte de algo mais concreto, não muito diferente da abordagem de Duncan Buell.

Buell, Duncan A. **Binary Quadratic Forms**. New York, NY: Springer-Verlag, 1989.

É notável também que formas quadráticas são relevantes em outros contextos. Cursos básicos de Álgebra Linear, por exemplo, tratam de propriedades algébricas e geométricas dessas formas, quando aplicadas sobre corpos (usualmente $\mathbb{R}$ ou $\mathbb{C}$), diferentemente da abordagem usual em Teoria dos Números, onde são aplicadas ao anel $\mathbb{Z}$.

$\lambda \in K$,

$$f(v + \lambda u, w) = f(v, w) + \lambda f(u, w)$$
$$f(v, u + \lambda w) = f(v, u) + \lambda f(v + w). \qquad \blacktriangleleft$$

Definição 11.2 (matriz de uma forma bilinear)**.** *Seja f uma forma bilinear em um espaço vetorial V com base $\{b_1, b_2, \ldots, b_n\}$. Então a **matriz da forma** f é a matriz de Gram*[2] *$m_{ij} = f(b_i, b_j)$:*

$$M = \begin{pmatrix} f(b_1, b_1) & f(b_1, b_2) & \ldots & f(b_1, b_n) \\ f(b_2, b_1) & f(b_2, b_2) & \ldots & f(b_2, b_n) \\ \vdots & & \ddots & \vdots \\ f(b_n, b_1) & f(b_n, b_2) & \cdots & f(b_n, b_n) \end{pmatrix}. \qquad \blacktriangleleft$$

Teorema 11.1. *Toda forma bilinear é determinada por sua matriz. Se a matriz de f é F, então*

$$f(x, y) = x^T F y.$$

Para demonstrar o Teorema 11.1 basta desenvolver $f(x, y)$ em somatórios representando x e y como combinações lineares da base do espaço, e chega-se a $f(x, y) = x^T F y$.

Definição 11.3 (forma bilinear simétrica)**.** *Uma forma bilinear f é **simétrica** se $f(x, y) = f(y, x)$.* $\blacktriangleleft$

Proposição 11.1. *Uma forma bilinear é simétrica se e somente se sua matriz é simétrica.*

Demonstração. A matriz da forma é simétrica se e somente se $f(b_i, b_j) = f(b_j, b_i)$. $\square$

Definição 11.4 (forma quadrática)**.** *Seja V um espaço vetorial de dimensão finita n. A **forma quadrática** associada a uma forma bilinear $f : V \times V \to K$ é $q(x) = f(x, x)$.*
*n é o **grau** da forma quadrática. Quando $n = 2$ a forma é chamada de **forma quadrática binária**, e usualmente escrevemos*

$$q(x, y) = ax^2 + bxy + cy^2.$$

Tratamos somente de formas quadráticas com coeficientes em $\mathbb{Z}$.
*Uma forma quadrática é **primitiva** se o polinômio que ela define é primitivo (ou seja, se o MDC de seus coeficientes é um).* $\blacktriangleleft$

[2] A matriz de Gram de n vetores é usualmente definida como a matriz onde o elemento na posição i, j é o produto interno do i-ésimo com o j-ésimo vetor. Uma forma bilinear pode não ser produto interno, porque $f(v, v)$ pode ser negativo, e porque $f(v, w)$ pode ser diferente de $f(w, v)$, mas ainda assim usamos o nome "matriz de Gram".

Exemplo 11.1. *A forma quadrática* $3x_1^2 - x_2^2 + x_3^2 - 2x_1x_2 + x_2x_3$ *é representada pela matriz*

$$\begin{pmatrix} 3 & -1 & 0 \\ -1 & -1 & 1/2 \\ 0 & 1/2 & 1 \end{pmatrix},$$

porque

$$\begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} \begin{pmatrix} 3 & -1 & 0 \\ -1 & -1 & 1/2 \\ 0 & 1/2 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = 3x_1^2 - x_2^2 + x_3^2 - 2x_1x_2 + x_2x_3.$$

Esta forma é primitiva, porque $\operatorname{mdc}(3, -1, 1, -2, 1) = 1$. ◀

Exemplo 11.2. *A forma quadrática* $6x^2 - 3xy + 9y^2$ *é representada pela matriz*

$$\begin{pmatrix} 6 & -3/2 \\ -3/2 & 9 \end{pmatrix}.$$

A forma não é primitiva, porque $\operatorname{mdc}(6, -3, 9) = 3$. ◀

A forma quadrática binária $ax^2 + bxy + cy^2$ é representada pela matriz

$$Q = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}.$$

O Teorema 11.2 define uma bijeção entre formas bilineares e e formas quadráticas.

Teorema 11.2. *Seja* q *uma forma quadrática em um espaço vetorial* V*, tal que* $q(x) = f(x, x)$*, onde* f *é uma forma bilinear.*
Se $1 + 1 \neq 0$ *no corpo subjacente*[3] *a* V*, então a forma bilinear* f *é única.*

Demonstração. Sejam $v, w \in V$. Então

$$\begin{aligned} q(v + w) &= f(v + w, v + w) \\ &= f(v, v) + 2f(v, w) + f(w, w) \\ &= q(v) + q(w) + 2f(v, w) \end{aligned}$$

e, como $2 \neq 0$ no corpo subjacente, o termo $2f(v, w)$ na expressão acima é diferente de zero, e temos

$$f(v, w) = \frac{q(v + w) - q(v) - q(w)}{2},$$

definida unicamente.

[3]Ou seja, se V tem característica diferente de 2. O Teorema não vale, por exemplo, em $\mathbb{Z}_2$, o corpo finito contendo apenas 0 e 1, e onde $1 + 1 = 0$.

□

Ou ainda,

$$f(v,w) = 2^{-1}\left(q(v+w) - q(v) - q(w)\right),$$

mas 2 (ou seja, $1+1$) somente tem inverso se a característica do corpo é diferente de 2.

Definição 11.5. *O **determinante** de uma forma quadrática é o determinante de sua matriz.* ◀

Exemplo 11.3. *A forma quadrática $3x^2 - 2xy - 2y^2$ tem matriz associada*

$$\begin{pmatrix} 3 & -1 \\ -1 & -2 \end{pmatrix},$$

cujo determinante é -7; dizemos que o determinante da forma $3x^2 - 2xy - 2y^2$ é -7. ◀

Uma forma quadrática pode assumir valores maiores, menores ou iguais a zero; quando a forma é definida em duas variáveis, visualizamos que algumas formas (as que tem discriminante[4] $\Delta < 0$) nunca cruzam o plano xy,

[4] Definiremos discriminante somente para formas quadráticas binárias, mas estes são usualmente definidos para o caso geral de polinômios. Uma possível definição, usando as raízes do polinômio, é: Seja $p(x) = a_n x^2 + \cdots + a_1 x + a_0$ um polinômio, e sejam $r_1, r_2, \ldots, r_n$ suas raízes. O discriminante de p é

$$\mathrm{Disc}(p) = a_n^{2n-2} \prod_{j<j} (r_j - r_i)^2.$$

Para $a^2x + bx + c$, por exemplo, temos o familiar discriminante

$$\begin{aligned} a^{4-2}(r_2 - r_1)^2 &= a^{4-2}\left(\frac{(-b + \sqrt{b^2 - 4ac}) - (b - \sqrt{b^2 - 4ac})}{2}\right)^2 \\ &= b^2 - 4ac. \end{aligned}$$

O termo "discriminante" foi usado inicialmente em 1851 por James Joseph Sylvester.

Sylvester, James Joseph. On a remarkable discovery in the theory of canonical forms and of hyperdeterminants. **Philosophical Magazine**, v. 4, n. 2, p. 391–410, 1851.

O termo é usado pela primeira vez na página 406, onde Sylvester inclui uma nota de rodapé justificando a escolha do nome:

> *"Discriminante", porque fornece o discernimento ou teste para determinar se fatores iguais entram em uma função de duas variáveis, ou de forma mais geral, a existência de múltiplos pontosno locus representado ou caracterizado por qualquer função algébrica, a mais óbvia e inicialmente observada espécie de singularidade in tal função ou locus. O progresso nessas pesquisas é impossível sem o auxílio de uma expressão clara; e a primeira condição de uma boa nomenclatura é que coisas diferentes sejam chamadas por nomes diferentes. As inovações na linguagem matemática aqui e em outros lugares (não sem alta sanção) introduzidas pelo autor, nunca foram adotadas exceto sob a experiência real do embaraço decorrente da falta delas, e não exigirão nenhuma vindicação para aqueles que*

e portanto seus valores são sempre positivos ou sempre negativos – dizemos que estas formas são *definidas positivas* ou *definidas negativas*. Uma forma quadrática que cruze o plano xy é *indefinida*. Outra maneira de expressar esse mesmo fato é: uma forma quadrática *definida positiva* tem valor positivo para quaisquer valores de x e y; uma forma quadrática *definida negativa*, similarmente, resultará somente em valores negativos; e as formas *indefinidas* resultam em valores positivos ou negativos, dependendo dos valores de x e y. Consolidamos estas idéia na Definição 11.6.

Definição 11.6 (formas definidas e indefinidas)**.** *Uma forma quadrática* f *é* ***positiva definida*** *quando* $f(x) = 0$ *implica em* $x = 0$*;* ***positiva semidefinida*** *quando* $f(x) \geq 0$ *para todos os valores de* x*; e* ***indefinida*** *quando pode assumir valores positivos e negativos.*

Formas quadráticas ***negativas definidas*** *e* ***negativas semidefinidas*** *são definidas de forma análoga às positivas.* ◄

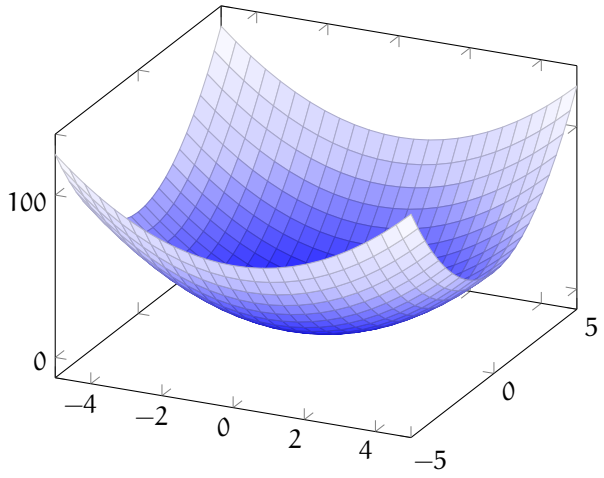
A forma $f(x, y) = 2x^2 + 3y^2$ é positiva definida, porque assume valores positivos para todos x, y exceto para $x = 0, y = 0$, quando seu valor é zero. A figura a seguir mostra o gráfico de f quando o domínio é estendido aos reais.

---

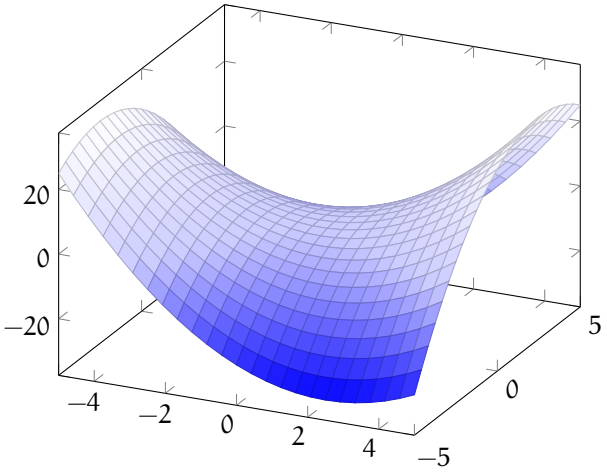
chegaram ao ponto em que a necessidade de algumas dessas adições se torna sentida.

> *"Discriminant", because it affords the discrimen or test for ascertaining wether or not equal factors enter into a function of two variables, or more generally of the existence or otherwise of multiple points in the locus represented or characterized by any algebraical function, the most obvious and first observed species of singularity in such function or locus. Progress in these researches is impossible without the aid of clear expression; and the first condition of a good nomenclature is that different things shall be called different names. The innovations in mathematical language here and elsewhere (not without high sanction) introduced by the author, have been never adopted except under actual experience of the embarassement arising from the want of them, and will require no vindication to those who have reached that point where the necessity of some such additions becomes felt.*

A definição que acabamos de dar permite perceber que o discriminante será zero se e somente se pelo menos duas raízes do polinômio forem iguais.



Já $g(x,y) = x^2 + xy - y^2$ é indefinida, porque $f(1,0) = 1$, e $f(0,1) = -1$. Da mesma forma que o gráfico anterior, o domínio foi estendido aos reais.



11.1.1 Representação de inteiros e equivalência de formas

Definição 11.7 (representação por forma quadrática; representação própria)**.** *Uma forma quadrática* f ***representa*** *um inteiro* n *se existe* $x = (x_1, \ldots, x_k)$ *tal que* $f(x) = n$*. Se* $\operatorname{mdc}(x_1, \ldots, x_k) = 1$ *dizemos que* f *é representação* ***própria*** *de* n*.* ◀

Exemplo 11.4. *A forma* $f(x,y) = 2x^2 - xy + 3y^2$ *representa, dentre outros,*

os inteiros $3, 4, 6$ *e* 29, 48, *porque*

$$\begin{aligned} f(0,1) &= 3 \\ f(1,1) &= 4 \\ f(-1,1) &= 6 \\ f(2,3) &= 29 \\ f(2,4) &= 48. \end{aligned}$$

O último número mostrado, 48, *tem representação imprópria, porque* $\operatorname{mdc}(2,4) = 2$. ◀

A forma, no entanto, não representa o inteiro -1, porque não existem x e y tais que $f(x,y) = -1$.

Definição 11.8 (formas quadráticas equivalentes)**.** *Duas formas quadráticas são* ***equivalentes*** *se se existe matriz unimodular* U *tal que*[5] $F = UGU^T$. *Escrevemos* $f \sim g$ *quando* f *é equivalente a* g. ◀

O Teorema 11.3 é apresentado sem sua demonstração, que é bastante simples.

Teorema 11.3. *A relação* $\sim$ *é de equivalência.*

O próximo teorema relaciona os conjuntos de números representados por formas.

Teorema 11.4. *Formas equivalentes representam os mesmos conjuntos de números inteiros.*

Demonstração. Suponha que $f \sim g$, e que portanto haja U unimodular tal que $F = UGU^T$.
$F(v) = n$ é o mesmo que $v(UGU^T)v^T = n$. Podemos reescrever $(vU)G(U^Tv^T) = n$, que significa que G representa n, porque $G(vU) = n$. □

Exemplo 11.5. *Sejam*

$$G = \begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix}, \quad U = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}, \quad F = \begin{pmatrix} 15 & 20 \\ 20 & 27 \end{pmatrix}.$$

É simples verificar que $\det F = \det G = 4$, *e que* $\det U = 1$, *e que* $F = UGU^T$. *As formas quadráticas* F *e* G, *portanto, são equivalentes, e representam os mesmos números.*

$$\begin{aligned} G(x,y) &= 3x^2 + 2xy + 2y^2 \\ F(x,y) &= 15x^2 + 40xy + 27y^2 \end{aligned}$$

[5] Isto é diferente de semelhança de matrizes. Temos UGU^T, e não UGU^{-1}, porque queremos preservar a invariante da simetria da forma, e não a transformação linear que ela representa, em base diferente.

Escolhemos um vetor, $(-2,3)$*. Então* $F(-2,3) = 15(-2)^2+40(-2)(3)+27(3)^2 = 63$*. O número 63 deve, portanto, ser representado por* G *também. Como apontado na demonstração do Teorema 11.4, se* $F = UGU^T$*, então* G *representa* n *porque* $G(vU) = n$*. Basta calcular* vU*, que neste caso é*

$$(-2,3)U = (-2,3)\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} = (1,5).$$

E realmente,

$$\begin{aligned} G(1,5) &= 3x^2 + 3xy + 2y^2 \\ &= 3(1) + 2(5) + 2(25) \\ &= 63, \end{aligned}$$

G *representa o número 63.* ◀

Corolário 11.1. *Se* $f \sim g$ *então as matrizes de* f *e* g *tem o mesmo determinante.*

Demonstração. Claramente, se $F = UGU^T$ e U é unimodular, os determinantes de F e G são iguais, porque $\det(UU^T) = 1$. □

Proposição 11.2. *Se* $f \sim g$ *então as matrizes de* f *e* g *tem o mesmo posto.*

O resto desta Seção trata da finitude da quantidade de classes de formas com o mesmo grau e determinante.

Teorema 11.5. *Para cada determinante* $D \neq 0$ *e grau* n *existe um número finito de classes de equivalência de formas quadráticas.*

Demonstração. □

11.2 Formas quadráticas binárias

Deste ponto adiante a discussão ficará restrita a formas quadráticas binárias integrais (ou seja, com matrizes tendo entradas em $\mathbb{Z}$).
O estudo de formas quadráticas foi sistematizado por Gauss, incluindo as idéias centrais desta seção (o discriminante como característica chave das formas, e o conceito de redução de formas)[6].

Definição 11.9 (forma quadrática binária)**.** *Uma* ***forma quadrática binária*** *é uma forma quadrática em duas variáveis. É usual denotar*[7] *uma forma* $ax^2 + bxy + cy^2$ *por* (a,b,c)*.* ◀

[6] No *Disquisitiones Arithmeticae.*

[7] A notação "(a,b,c)" foi introduzida por Gauss no segundo parágrafo do artigo 153 (o primeiro da seção V) do *Disquisitiones.*

Definição 11.10 (discriminante)**.** *O* ***discriminante*** *de uma forma quadrática* $ax^2 + bxy + cy^2$ *é* $\Delta = b^2 - 4ac$. ◀

Como $\Delta_A = -4 \det A$, podemos dizer que formas equivalentes tem o mesmo discriminante, ou ainda, que o discriminante é uma *invariante* das formas quadráticas, conforme a Definição 11.11.

Definição 11.11. *Seja* s *uma função definida sobre os coeficientes de uma forma quadrática. Se* $f = (a, b, c) \sim g = (A, B, C)$ *implica que* $s(a, b, c) = s(A, B, C)$ *dizemos que* s *é uma* ***invariante*** *de formas quadráticas.* ◀

O Teorema 11.6 implica que não há formas quadráticas binárias com discriminante $4k + 2$ ou $4k + 3$.

Teorema 11.6. *O discriminante de uma forma quadrática sempre é congruente a zero ou um módulo* 4*, ou seja,* Δ *é da forma* $4k$ *ou* $4k + 1$*.*
Além disso, se um inteiro Δ *é da forma* $4k$ *ou* $4k + 1$*, há pelo menos uma forma quadrática com discriminante* Δ*.*

Demonstração. Para ver que Δ é da forma dada, basta analisar $b^2 - 4ac \pmod 4$. $4ac$ sempre é congruente a 0 módulo 4, portanto Δ será congruente a b^2 módulo 4, mas quadrados somente deixam resto um ou zero módulo 4. Se $\Delta \equiv 0 \pmod 4$ então

$$x^2 - \frac{\Delta}{4} y^2$$

tem discriminante Δ. Da mesma forma, se $\Delta \equiv 1 \pmod 4$, então

$$x^2 + xy - \frac{\Delta - 1}{4} y^2$$

terá discriminante Δ. □

Por haver mais de uma forma com o mesmo discriminante, e será interessante definir qual forma será representante natural do conjunto. Da demonstração acima extraímos o conceito de *forma principal*, na Definição 11.12.

Gauss, Johann Carl Friedrich. **Disquisitiones Arithmeticae**. [*S. l.*], 1801.

> *Representamos a forma* $ax^2 + 2bxy + cy^2$ *pelo símbolo* (a, b, c) *quando não estivermos interessados nas incógnitas* x, y.
>
> *Formam* $axx + 2bxy + cyy$ *quando de indeterminatis* x, y *non agitur, ita designabimus,* (a, b, c).

Vemos que Gauss usava "$2bxy$", e não "bxy".

Definição 11.12 (forma principal)**.** *A* ***forma principal*** *de um discriminante* Δ *é*

$$\left(1, 0, \frac{-\Delta}{4}\right) \text{ se } \Delta \equiv 0,$$
$$\left(1, 1, \frac{-(\Delta-1)}{4}\right) \text{ se } \Delta \equiv 1. \qquad \blacktriangleleft$$

Exemplo 11.6. *A forma principal para o discriminante* -8 *é* $(1,0,2)$*, ou* x^2+2y^2*; a forma principal para o discriminante* -17 *é* $(1,1,4)$*, ou* x^2+4y^2*; para o discriminante* 12*, é* $(1,0,-3)$*, ou* x^2-3y^2*.* $\blacktriangleleft$

Embora formas equivalentes tenham o mesmo determinante e discriminante, a recíproca não vale:

$$F = \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}, \quad G = \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}$$

As duas formas tem o mesmo discriminante $\Delta = -20$, e o mesmo determinante ($\det F = \det G = 52$), mas não são equivalentes: F representa 1: $F(1,0) = 1$, mas G não representa 1, porque

$$G(x,y) = 2x^2 + 2xy + 3y^2,$$

que sempre será estritamente maior que um.

Teorema 11.7. *Seja* $f(x,y) = ax^2+bxy+cy^2$ *uma forma quadrática com discriminante* Δ*. Esta forma é indefinida se* $\Delta > 0$*; semidefinida (mas não definida) se* $\Delta = 0$*; e definida quando* a *e* c *tiverem o mesmo sinal, e* $\Delta < 0$*. Quando a forma é definida, será positiva quando* $a > 0$ *e negativa quando* $a < 0$ *.*

Teorema 11.8. *Uma forma quadrática binária é produto de duas formas lineares se e somente se seu discriminante é quadrado perfeito.*

Demonstração. Se $a = 0$ então a forma é $bxy + cy^2$ e o discriminante é b^2. Mas $bxy + cy^2 = y(bx + cy)$, produto de duas formas lineares.
Presumiremos no resto da demonstração que $a \neq 0$.
Seja $\Delta = b^2 - 4ac$ o discriminante da forma. Observamos que

$$4a\, f(x,y) = (2ax + by)^2 - \Delta y^2,$$

Se Δ é quadrado – por exemplo, $\Delta = z^2$ – então

$$4af(x,y) = (2ax + (b-z)y)(2ax + (b+z)y)$$
$$f(x,y) = \frac{(2ax + (b-z)y)(2ax + (b+z)y)}{4a},$$

e f é produto de dois fatores lineares racionais, ou seja, há $k, m \in \mathbb{Z}$ tal que

$$\begin{aligned} f(x,y) &= \frac{k}{m} p(x,y) q(x,y) \\ df(x,y) &= k p(x,y) q(x,y), \end{aligned}$$

com $k, m > 0$ e $\operatorname{mdc}(k,m) = 1$.
Pelo Lema 5.10 (lema de Gauss[8]), $c(pq) = c(p)\,c(q)$ e portanto

$$\begin{aligned} m f(x,y) &= k p(x,y) q(x,y) \\ m\, c(f) &= k \end{aligned}$$

Como $\operatorname{mdc}(k,m) = 1$, $m = 1$, e f é produto de duas formas lineares. □

Exemplo 11.7. *A forma $2x^2 - xy - y^2$ tem discriminante $(-1)^2 - 4(2)(-1) = 9$, quadrado perfeito, e pode se decomposta em $(2x + y)(x - y)$.* ◀

Teorema 11.9. *Um número $n \in \mathbb{Z}$ tem representação própria por uma forma quadrática binária $f(x,y)$ se e somente se é coeficiente de x^2 em alguma forma equivalente a f.*

Demonstração. Primeiro, mostramos que se um número é coeficiente de x^2 em uma forma equivalente a f, ele tem representação própria por f.
Seja $f = ax^2 + bxy + cy^2$, e seja $f \sim g = \alpha x^2 + \beta xy + \gamma y^2$, tal que exista U unimodular com $G = UFU^T$:

$$\begin{pmatrix} \alpha & \beta/2 \\ \beta/2 & \gamma \end{pmatrix} = \begin{pmatrix} m & n \\ r & s \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} m & r \\ n & s \end{pmatrix}$$

Mas expandindo o produto das três matrizes obtemos

$$\alpha = am^2 + bmn + cn^2,$$

ou seja, $\alpha = f(m,n)$, e como a U é unimodular, $ms - nr = 1$, e $\operatorname{mdc}(m,n) = 1$. Esta representação de α por f é própria.
Agora suponha que $\alpha \in \mathbb{Z}$ é representável propriamente por f, ou seja, existem $m, n \in \mathbb{Z}$ tais que $f(m,n) = \alpha$. Provaremos que α é coeficiente de m^2 em alguma forma equivalente a f. Devem existir r, s tais que $ms - nr = 1$, e portanto existe uma matriz unimodular U tal que $F = UGU^T$:

$$\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} = \begin{pmatrix} m & n \\ r & s \end{pmatrix} \begin{pmatrix} \alpha & \beta/2 \\ \beta/2 & \gamma \end{pmatrix} \begin{pmatrix} m & r \\ n & s \end{pmatrix}$$

[8] **Lema 5.10 (de Gauss):** Sejam f, g são polinômios com coeficientes em um domínio Euclideano, nenhum deles nulo. Então $c(fg) = c(g)\,c(f)$. Assim, se f e g são primitivos, então fg também é.
Aqui $c(p)$ é o **conteúdo** do polinômio, definido como o MDC de seus coeficientes.

Novamente expandimos o produto no lado direito da equação para verificar que a, coeficiente de x^2 em g, será α:

$$a = \alpha m^2 + \beta mn + \gamma n^2. \qquad \square$$

Exemplo 11.8. *A forma* $f(x, y) = -3x^2 + xy - y^2$ *representa o número* -9*, porque* $f(-1, 2) = -9$*. Esta forma tem matriz*

$$F = \begin{pmatrix} -3 & 1/2 \\ 1/2 & -1 \end{pmatrix}.$$

A matriz F *pode ser transformada em* $G = UFU^T$ *com* $U = \begin{pmatrix} 1 & 3 \\ 1 & 4 \end{pmatrix}$*, e obteremos*

$$G = \begin{pmatrix} -9 & -23/2 \\ -23/2 & -15 \end{pmatrix}$$

que representa a forma $g(x, y) = -9x^2 - 23xy - 15y^2$*, com* -9 *no coeficiente de* x^2*.* ◀

O Teorema 11.10 e o Corolário11.2 conectam formas quadráticas binárias com a teoria de resíduos quadráticos.

Teorema 11.10. *Sejam* $n \neq 0$ *e* Δ *inteiros. Então há uma forma quadrática binária que representa propriamente* n*, com discriminante* Δ*, se e somente se* Δ *é resíduo quadrático módulo* $4|n|$*.*

Demonstração. Seja $f = (a, b, c)$.
Se f representa propriamente n, então $f(x, y) = n$, com $\mathrm{mdc}\,(x, y) = 1$. Pelo Teorema 11.9, existe $g \sim f$ com $g(x, y) = nx^2+, sxy+, ty^2$. Como f e g tem o mesmo discriminante,

$$\begin{aligned} \Delta &= s^2 - 4nt \\ \Delta &\equiv s^2 \pmod{4nt} \\ \Delta &\equiv s^2 \pmod{4|n|} \end{aligned}$$

Ou seja, o discriminante de f é quadrado módulo $4|n|$.
Para a recíproca, suponha que exista k tal que $k^2 \equiv \Delta \pmod{4|n|}$. Existe então r tal que $\Delta = k^2-4|n|r$. A forma $g = |n|x^2+kxy+ry^2$ tem discriminante $k^2 - 4|n|r = \Delta$, e $g(1, 0)$ é representação própria de n. $\square$

Corolário 11.2. *Seja* Δ *congruente a* 1 *ou* 0 *módulo* 4 *e* p *um primo ímpar. Então existe uma forma quadrática binária com discriminante* Δ *que representa* p *se e somente se* Δ *é diferente de zero e resíduo quadrático módulo* p*.*

Demonstração. Como p é primo, qualquer representação sua é própria, e pelo Teorema 11.10, Δ é quadrado módulo $4p$. Assim, $(\Delta/p) = 1$. A recíproca: se $(\Delta/p) = 1$ então Δ é resíduo quadrático módulo p. O enunciado determina que $\Delta \equiv 0, 1 \pmod 4$, o que significa que Δ é quadrado módulo 4 (porque um inteiro é quadrado módulo 4 se e somente se é congruente a 0 ou 1 módulo 4). Pelo Teorema Chinês dos Restos, como p é ímpar e

$$\begin{aligned} \Delta &\equiv r^2 \pmod p \\ \Delta &\equiv k^2 \pmod 4, \end{aligned}$$

Δ é quadrado módulo $4p$, e portanto, pelo Teorema 11.10, p tem representação própria por alguma forma com discriminante Δ. □

A Lei da Reciprocidade Quadrática define para quais primos ímpares $(\Delta/p) = 1$, sendo assim relevante para determinar que primos são representáveis por um dado discriminante.

Proposição 11.3. *Não há formas quadráticas binárias primitivas equivalentes a formas não-primitivas.*

Definição 11.13 (discriminante fundamental)**.** *Δ é um **discriminante fundamental** se todas as formas com discriminante Δ são primitivas.* ◀

Teorema 11.11. *Os discriminantes fundamentais são*

i) $\Delta = 4k + 1$ *livre de quadrados;*

ii) $\Delta = 4k$*, com* k *igual a* $4r + 2$ *ou* $4r + 3$*.*

Demonstração. Seja algum Δ como definido no enunciado, e suponha (por absurdo) que Δ seja discriminante de uma forma não primitiva $ax^2 + bxy + cy^2$. Seja $k = \operatorname{mdc}(a, b, c)$. Claramente, $k^2 | \Delta$, portanto Δ precisa ser to tipo (ii). A única possibilidade, portanto, é $\Delta = 2$. Isso implica que $a = 2\alpha$, $b = 2\beta$, $c = 2\gamma$, e $\Delta' = \Delta/4 = \beta^2 - 4\alpha\gamma$. Então $\Delta' = 4k$ ou $4k + 1$, o que é impossível, porque determinamos que Δ é to dipo (ii). Presumimos portanto que se Δ é de um dos dois tipos dados, não pode ser discriminante de uma forma não primitiva.
A recíproca: Suponha agora que Δ *não* seja como definido no enunciado. Tratamos dois casos: se $\Delta = 4k + 1$, tendo um quadrado como fator, então $\Delta = \Delta' m^2$, e a forma

$$mx^2 + mxy - \left(\frac{m(\Delta - 1)}{4}\right) y^2$$

tem discriminante Δ, mas claramente não é primitiva, porque m divide todos os coeficientes.

Se $\Delta = 4k$, verificamos três casos, k livre de quadrados; $k = 4r$; e $k = 4r+1$. Para os dois primeiros, a forma

$$mx^2 - \frac{k}{m}y^2 2$$

tem discriminante Δ e não é primitiva, porque m divide os dois coeficientes não nulos.
Se $k = r + 1$, a forma

$$2x^2 + 2xy - \frac{k-1}{2}$$

tem discriminante Δ e não é primitiva, porque 2 divide todos os coeficientes. Assim, se Δ como no enunciado, qualquer forma que o tenha como discriminante é não-primitiva. □

11.2.1 Redução de formas

Como cada forma pode ser equivalente a várias outras, é interessante definir algum critério para determinar que uma forma é "reduzida". Veremos que para classes de formas definidas positivas, a forma reduzida é única, e portanto pode ser usada para comparar formas: para saber se duas formas f e g estão na mesma classe de equivalência, basta reduzir ambas e verificar se a forma reduzida das duas é a mesma.
Primeiro mostraremos que qualquer forma (a, b, c) é equivalente a outra forma (A, B, C) com $|B| \leq |A| \leq |C|$, e depois usaremos esta propriedade para definir forma reduzida, mas apenas para formas definidas positivas.

Lema 11.1. *Dados $a, b, c, k \in \mathbb{Z}$, então*

i) $(a, b, c) \sim (c, -b, -a)$, *e*

ii) $(a, b, c) \sim (a, b + 2ka, ak^2 + bk + c)$.

Demonstração.

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad T^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$$

são unimodulares, e levam (a, b, c) às duas formas equivalentes dadas no enunciado:

$$S^T F S = (c, -b, a)$$
$$(T^k)^T F T^k = (a, b + 2ka, ak^2 + bk + c) \qquad \square$$

Note que se $|a| > |c|$, a transformação S leva a uma forma (A, B, C) com $|A| < |C|$, porque troca a posição dos dois argumentos. Se $|b| > |a|$, a pode-se escolher k tal que a transformação T^k leva a uma forma (A, B, C) com

$|B| < |A|$. Assim, se uma forma (a, b, c) não é como desejado, o Lema 11.1 permite encontrar uma forma equivalente (A, B, C) em que $|A| \leq |C|$ ou $|B| \leq |A|$. Após uma quantidade finita de passos, chega-se a uma forma em que os coeficientes tem a propriedade que queremos:

1. Se $|a| > |c|$, troque (a, b, c) por $(c, -b, -a)$ (use S);

2. Se $|b| > |a|$, troque (a, b, c) por (a, B, C), onde $B = b + 2ak$, com k escolhido tal que $|B| \leq |a|$ (use T^k);

3. Se a forma obtida não for tal que $|b| \leq |a| \leq |c|$, repita os dois passos anteriores.

Teorema 11.12. *Em cada classe de equivalência relacionada a um discriminante que não seja quadrado perfeito existe pelo menos uma forma com* $|b| \leq |a| \leq |c|$.

Demonstração. Iniciando com uma forma qualquer (a, b, c) na classe de equivalência, basta aplicar o algoritmo descrito no parágrafo anterior ao enunciado. O algoritmo necessariamente para, e chega a uma forma com $|b| \leq |a| \leq |c|$. □

Definiremos *para formas definidas positivas* o conceito de forma reduzida. Para as formas indefinidas o algoritmo apresentado funciona, mas pode haver mais de uma forma com a caracterização dada; o tratamento de formas indefinidas é usualmente feito de maneira diferente, e não o abordaremos.

Definição 11.14 (forma quadrática positiva definida reduzida e semirreduzida)**.** *Uma forma quadrática positiva definida* (a, b, c) *é* ***semirreduzida*** *se* $|b| \leq a \leq c$*;* ***reduzida*** *se*

i) $-a \leq b < a < c$, *ou*

ii) $0 \leq b \leq a = c$. ◀

Teorema 11.13. *Se duas formas semirreduzidas são equivalentes, então elas são*

i) $(a, b, a) \sim (a, -b, a)$ *ou*

ii) $(a, a, c) \sim (a, -a, c)$.

Demonstração. Sejam $f = (a, b, c) \sim g = (A, B, C)$. Então existe $U = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$, unimodular, tal que $G = UFU^T$. Mostramos inicialmente que $a = A$: suponha, sem perda de generalidade, que $A \leq a$. A transformação determina

que

$$\begin{aligned} A &= ar^2 + brt + ct^2 \\ B &= s(2ar + bt) + u(2ct + br) \\ C &= as^2 + bsu + cu^2. \end{aligned}$$

Suponha, sem perda de generalidade, que $a \geq A$.

$$\begin{aligned} a &\geq A \\ &\geq ar^2 - a|rt| + at^2 \\ &= a|rt| + a(|r| - |t|)^2 \\ &\geq a|rt|, \end{aligned}$$

e $a \geq A \geq a|rt|$. $|rt|$ deve ser, portanto menor ou igual que um, ou teríamos $a \geq a|rt| > a$. Mas r e t não podem ser ambos zero, porque dessa forma teríamos U com determinante zero. As possibilidades para r e t são $(0, \pm 1)$, $(\pm 1, 0)$, $(\pm 1, \pm 1)$, $(\pm 1, \mp 1)$.

Também comcluímos que quando r, t são ambos diferentes de zero, $a \geq A \geq a|rt|$ e $|rt| = 1$ implicam que $a = A$.

O mesmo raciocínio aplicado usando $c \geq C$ leva à conclusão de que na segunda coluna de U, as possibilidaes de valores para s e u são as mesmas. Além disso, para que $\det U = 1$, se $r = 0$ ou $u = 0$, então $t = -s$, e se $s = 0$ ou $t = 0$, $u = r$.

Dividimos as matrizes integrais com estas restrições em três casos, de acordo com a primeira coluna. Note que nos dois primeiros casos a primeira coluna igual a $(1, 0)$ ou $(0, 1)$ determina um dos elementos da segunda, para que o determinante seja 1.

$$\begin{aligned} \pm \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}, &\quad (a, b, c) \to (a, b \pm 2as, \ldots) \\ \pm \begin{pmatrix} 0 & -1 \\ 1 & u \end{pmatrix}, &\quad (a, b, c) \to (c, b \pm 2au, \ldots) \\ \pm \begin{pmatrix} 1 & s \\ \pm 1 & u \end{pmatrix}, &\quad (a, b, c) \to (a \pm b + c, \ldots, \ldots) \end{aligned}$$

Os valores de s e u devem ser 0 ou ± 1, e no terceiro caso exatamente um deles deve ser zero.

No primeiro caso, se $s = 0$ a matriz é a identidade; quando $s = 1$, $b \pm 2as = b \pm 2a$ e a desigualdade $|b \pm 2a| \leq |a|$ só é possível com $a = -b$, e teremos $(a, a, c) \to (a, -a, c)$. Quando $s = -1$, $a = b$ e a transformação é $(a, -a, c) \to (a, a, c)$.

No segundo caso, a transformação determina que o primeiro coeficiente

passa a ser c. Como as duas formas são semirreduzidas, $a \leq c \leq a$ implica que $a = c$ e $f = (a, b, a)$. Se $u = 0$, a transformação leva de (a, b, a) em $(a, -b, a)$. Se $u = 1$, a transformação é $(a, b, a) \to (a, -b \pm 2a, \dots)$, mas é necessário que $|-b + 2a| \leq |a|$, o que só é possível se $a = b$, e temos $(a, a, a) \to (a, -a, a)$. Quando $u = -1$, $a = -b$ e a transformação é $(a, -a, a) \to (a, a, a)$.
No último caso, o primeiro coeficiente de g é $a + b + c$, mas como r e t são diferentes de zero, $a = A$ e $b = -c$. Como as duas formas são semirreduzidas, $a = \pm b$, $f = (a, a, a)$ ou $f = (a, -a, a)$. As matrizes do terceiro caso representam as transformações $(a, a, a) \to (a, -a, a)$, $(a, -a, a) \to (a, a, a)$, $(a, a, a) \to (a, a, a)$ e $(a, -a, a) \to (a, -a, a)$. □

Corolário 11.3. *Uma classe de equivalência de formas quadráticas definidas positivas tem uma e somente uma forma reduzida.*

Lema 11.2. *Se (a, b, c) é uma forma semirreduzida positiva definida com discriminante Δ, então*

$$0 < a < \sqrt{\frac{-\Delta}{3}}.$$

Demonstração. Como a forma é semirreduzida, $a > 0$ e $\Delta < 0$. Mas $ac \geq a^2$, porque $c \geq a$. Além disso, $b^2 < a^2$, porque $|b| < a$. Com isso temos

$$\begin{aligned} -\Delta &= -b^2 + 4ac \\ &\geq -a^a + 4a^2 \\ &= 3a^2. \end{aligned}$$

□

O Teorema 11.14 ilustra como formas quadráticas simplificam demonstrações.

Teorema 11.14. *Toda forma quadrática binária definida positiva com discriminante -4 é equivalente a uma soma de dois quadrados.*

Demonstração. Se o discriminante de f é $\Delta_f = -4$, então seja g, semirreduzida, tal que $f \sim g = (a, b, c)$, evidentemente com $\Delta_g = -4$. Pelo Lema 11.2,

$$\begin{aligned} a &\leq \sqrt{\frac{-\Delta_g}{3}} \\ &= \sqrt{\frac{4}{3}} \\ &= \frac{2}{\sqrt{3}} < 2. \end{aligned}$$

Como $a > 0$, necessariamente precisamos $a = 1$. Mas b deve ser zero ou um, porque $|b| < a$. Como[9] $b^2 \equiv \Delta_g \equiv 0 \pmod 4$, então $b = 0$. Com isso c fica determinado:

$$\begin{aligned}\Delta_g &= b^2 - 4ac \\ -4 &= 0 - 4(1)c\end{aligned}$$

e $c = 1$. Então, $g = (1, 0, 1)$, ou seja,

$$g(x, y) = x^2 + y^2,$$

uma soma de dois quadrados. □

11.2.2 Quantidade de representações

Um automorfismo de uma forma quadrática f é uma bijeção a que preserva f – ou seja,

$$f(v) = f(a(v)).$$

No entanto, isto **não** se traduz em "uma matriz A tal que $AF = F$", porque a aplicação da forma quadrática no vetor v ocorre por duas multiplicações, nos dois lados de F: se $v = (x, y)^T$,

$$\begin{aligned}f(x, y) &= f(a(x, y)) \\ (v^T)F(v) &= (Av)^T F(Av) \\ &= (v^T A^T)F(Av) \\ &= v^T \ \ (A^T F A) \ \ v\end{aligned}$$

A maneira usual de escrever este fato é $\exists A : \quad F = AFA^T$ (equivalente a $\exists A : \ F = A^T F A$, que identificamos acima).
O automorfismo claramente será unimodular, de outra forma o determinante de F será modificado.
Intuitivamente, um "automorfismo" de f é a matriz que pode ser usada para mostrar que f é equivalente a si mesma (ou seja, que f é *isomorfa* a si mesma – e um isomorfismo de um objeto nele mesmo é um automorfismo).

Definição 11.15 (automorfismo de forma quadrática)**.** *Seja f uma forma quadrática com matriz F. Um **automorfismo** de f é uma matriz integral*[10]

[9] Conforme a demonstração do Teorema 11.6:
Teorema 11.6: O discriminante de uma forma quadrática sempre é congruente a zero ou um módulo 4, ou seja, Δ é da forma $4k$ ou $4k + 1$.
Além disso, se um inteiro Δ é da forma $4k$ ou $4k + 1$, há pelo menos uma forma quadrática com discriminante Δ.

[10] Pode-se definir o automorfismo como matriz não necessariamente integral, mas neste contexto, onde há o objtivo de contar quantidades de automorfismos, é essencial que as matrizes somente tenham entradas integrais.

(e unimodular) U *tal que* $UFU^T = F$.
A ***quantidade de automorfismos*** *de* f *é denotada por* $w(f)$. ◀

Exemplo 11.9. *Seja* $f = (2, -1, 1)$. *A matriz de* f *é* $F = \begin{pmatrix} 2 & -1/2 \\ -1/2 & 1 \end{pmatrix}$. *Um automorfismo de* F *é* $U = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}$, *porque*

$$UFU^T = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & -1/2 \\ -1/2 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix} = F. \qquad \blacktriangleleft$$

A quantidade de automorfismos para cada forma definida positiva é limitada.

Teorema 11.15. *Os automorfismos de uma forma quadrática binária positiva definida reduzida* f *são exatamente*

$$\begin{cases} x = \pm X \\ y = \pm Y \end{cases} \quad \begin{cases} x = \pm X \\ y = \mp Y \end{cases} \qquad \text{se } f = (a, 0, a)$$

$$\begin{cases} x = \pm X \\ y = \pm Y \end{cases} \quad \begin{cases} x = \pm X \\ y = \mp X \mp Y \end{cases} \quad \begin{cases} x = \pm X \pm Y \\ y = \mp X \end{cases} \qquad \text{se } f = (a, a, a)$$

$$\begin{cases} x = \pm X \\ y = \pm Y \end{cases} \qquad \text{em outros casos,}$$

e portanto $w(f)$ *pode ser* 4, 6 *ou* 2, *conforme os casos acima.*

Demonstração. Lembramos, do Teorema 11.1[11], que

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

O Teorema 11.13[12] determina as equivalências possíveis entre formas semireduzidas. Para selecionar os automorfismos, eliminamos $(a, a, c) \to (a, -a, c)$, porque a única forma que esta transformação leva em si mesma é $(a, -a, a)$, que é semirreduzida mas não reduzida. Para o caso $(a, b, a) \to (a, -b, a)$, é necessário que $b = 0$ ou $b = a$. Portanto, dentre as transformações listadas naquele Teorema as seguintes são automorfismos:

- $\pm I$, duas possibilidades para o caso geral;

[11] **Lema 11.1:** Dados $a, b, c, k \in \mathbb{Z}$, então
i) $(a, b, c) \sim (c, -b, -a)$, e
ii) $(a, b, c) \sim (a, b + 2ka, ak^2 + bk + c)$.

[12] **Teorema 11.13:** Se duas formas semirreduzidas são equivalentes, então elas são
i) $(a, b, a) \sim (a, -b, a)$ ou
ii) $(a, a, c) \sim (a, -a, c)$.

- $\pm S$ é automorfismo para $(a, 0, a)$, e para estas formas temos mais duas possibilidades, totalizando quatro.
- As transformações $\pm ST = \pm \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ e $\pm (ST)^2 = \pm \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$, também dentre aquelas listadas no Teorema 11.13, levam (a, a, a) em (a, a, a). Assim, além das duas transformações $\pm I$, há mais quatro, totalizando seis.

Todas as outras transformações entre formas reduzidas necessariamente modificam a forma.
As transformações identificadas, quando aplicadas a $\begin{pmatrix} X \\ Y \end{pmatrix}$, resultam nas trocas de variáveis listadas no enunciado. □

Corolário 11.4. *Se f é uma forma primitiva positiva com discriminante Δ, então*

$$w(f) = \begin{cases} 6 & \text{se } \Delta = -3, \\ 4 & \text{se } \Delta = -4, \\ 2 & \text{se } \Delta < -4. \end{cases}$$

11.2.3 Número de classe

Além do número de representações de um inteiro, nos interessa a quantidade de classes de equivalência existentes para cada determinante[13].

Definição 11.16 (número de classe)**.** *O **número de classe** de um discriminante fundamental Δ, denotado $h(\Delta)$, é o número de classes de equivalência próprias de formas primitivas com tal discriminante.* ◀

Exemplo 11.10. *Para o discriminante $\Delta = -15$ há apenas duas classes de equivalência:*

$$q(x, y) = x^2 + xy + 4y^2 = (1, 1, 4),$$
$$r(x, y) = 2x^2 + xy + 2y^2 = (2, 1, 2),$$

e estas não são equivalentes. Assim, $h(-15) = 2$. ◀

Há apenas cinco discriminantes negativos e múltiplos de 4 com número de classe igual a um: o Teorema11.16 determina isto (o passo final é pedido no Exercício 316).

Teorema 11.16. *Seja $n \in \mathbb{N}$. Então $h(-4n) = 1$ se e somente se n é $1, 2, 3, 4$ ou 7.*

[13] O conceito de número de classe foi introduzido por Gauss no *Disquisitiones Arithmeticae*.

Demonstração. Separamos a prova em duas partes.
Parte I: usamos desigualdades para mostrar que a forma principal é a única possível com o discriminante dado.
A forma equivalente, se existisse, poderia ser reduzida – então presumimos que a forma é reduzida, para podermos usar desigualdades.
Usaremos o Lema[14] 11.2 para determinar o valor máximo de a.

$n = 1$ Para $n = 1$, $\Delta = -4$, e a forma principal é $(1, 0, 1)$. Então $a < \sqrt{4/3}$, e precisa ser 1. Pelo Teorema[15] 11.13, a única forma equivalente seria $(1, -0, 1)$, que é a mesma forma.

$n = 2$ Para $n = 2$, $\Delta = -8$, e a forma principal é $(1, 0, 2)$. Então $a \leq \sqrt{8/3}$, e também precisa ser um. Pelo Teorema 11.13, não há forma equivalente.

$n = 3$ Para $n = 3$, $\Delta = -12$, e a forma principal é $(1, 0, 3)$. $a \leq \sqrt{12/3} = 2$, Mas se $a = 2$, precisamos de $b < a < c$, e teríamos $|b| < 2 < c$.

$$\begin{aligned} b^2 - 4ac &= b^2 - 8c \\ &< 1 - 8c && (b < 2,\ b = 1) \\ &< 1 - 8(3) && (2 < c, \text{ logo } c \geq 3) \\ &= -23. \end{aligned}$$

Não há, portanto, forma equivalente a $(1, 0, 3)$ com discriminante -12.

$n = 4$ Para $n = 4$, $\Delta = -16$, e a forma principal é $(1, 0, 4)$. $a \leq \sqrt{16/3} = 2$, Mas se $a = 2$, exatamente como no caso anterior, o discriminante é menor que -23 e não pode haver forma equivalente a $(1, 0, 4)$.

$n = 7$ Para $n = 7$, $\Delta = -28$, e a forma principal é $(1, 0, 7)$. $a \leq \sqrt{28/3} = 3$, Mas se $a = 3$,

$$\begin{aligned} b^2 - 4ac &= b^2 - 12c \\ &< 4 - 12c && (b < 3) \\ &< 4 - 12(4) && (3 < c, \text{ logo } c \geq 4) \\ &= -44. \end{aligned}$$

[14] **Lema 11.2:** Se (a, b, c) é uma forma semirreduzida positiva definida com discriminante Δ, então

$$0 < a < \sqrt{\frac{-\Delta}{3}}.$$

[15] **Teorema 11.13:** Se duas formas semirreduzidas são equivalentes, então elas são

i) $(a, b, a) \sim (a, -b, a)$ ou

ii) $(a, a, c) \sim (a, -a, c)$.

Se $a = 2$,

$$\begin{aligned} b^2 - 4ac &= b^2 - 8c \\ &\leq 1 - 8c && (b < 2,\ b \leq 1) \\ &\leq 1 - 8(3) && (2 < c, \text{ logo } c \geq 3) \\ &= -23. \end{aligned}$$

No entanto, a forma $(2, 1, 3)$ tem discriminante -23. Se tentarmos $(2, 0, c)$, o discriminante seria

$$0^2 - 4(2)c,$$

que não pode ser -28.

Assim, não há formas equivalentes às mencionadas.
Parte II: mostramos que quando n não é um dos números no enunciado, há pelo menos uma forma equivalente à principal.

$n = 5$ Para $n = 5$, temos $-4n = -20$, e a forma principal é $(1, 0, \frac{20}{4}) = (1, 0, 5)$ A forma $(2, 2, 3)$ é equivalente a essa, e $h(-20) > 1$.

$n = 6$ Para $n = 6$, temos $-4n = -24$, e a forma principal é $(1, 0, \frac{24}{4}) = (1, 0, 6)$. A forma $(2, 0, 3)$ é equivalente a essa, e $h(-24) > 1$.

$n \geq 8$ Para $n \geq 8$, a forma principal será $(1, 0, n)$. Podemos construir uma forma positiva definida primitiva e reduzida que não seja equivalente a $(1, 0, n)$.

i) Se n não é primo, seja d um divisor de n. Então $(d, 0, n/d)$ é equivalente à forma principal $(1, 0, n)$, e $h(-4n) > 1$.

ii) Se a forma é $(1, 0, p)$, com p primo: Exercício 316. □

11.2.4 O grupo de classes

Há uma quantidade de formas para cada discriminante, e uma pergunta natural é: "Há alguma maneira de combinar estas formas quadráticas? Elas formam alguma estrutura algébrica interessante?" E de fato, formam um grupo.
Gauss propôs em 1801 (antes do conceito de grupo ser formalizado) uma regra de composição de formas[16]. A regra de Gauss foi posteriormente

[16] No Disquisitiones, artigos 234 até 244.

> *234. Após termos apresentado preliminarmente a distribuição de formas em classes, genera e ordens, e explicando as propriedades gerais que decorrem dessas distinções, passamos a outro assunto muito importante, nunca abordado antes por ninguém: a composição de formas.*

simplificada por Dirichlet[17] em 1851.
Inicialmente, a regra de Gauss definia composição usando produto de polinômios. Venkov (Venkov, 1970) comenta:

> *Se as formas*
>
> $$F(X,Y) = AX^2 + 2BXY + CY^2,$$
> $$f(x,y) = ax^2 + 2bxy + cy^2,$$
> $$f'(x',y') = a'x'^2 + 2b'x'y' + c'y'^2,$$
>
> *são tais que, substituindo* X, Y *pelas expressões bilineares*
>
> $$X = pxx' + p'xy' + p''yx' + p'''yy'$$
> $$Y = qxx' + q'xy' + q''yx' + q'''yy'$$
>
> *obtivermos, identicamente em* x, y, x', y',
>
> $$F(X,Y) = f(x,y)f'(x',y')$$
>
> *então é dito que a forma* F *é transformável em um produto de formas* f, f' *(transformabilis in productum).*

Com mais alguns requisitos relacionados aos coeficientes $p, p', \ldots, q'''$, define F como a composição de f e f'.
A regra original e as conclusões derivadas por Gauss são descrita por no mesmo texto por Venkov (Venkov, 1970); a regra que damos aqui, é semelhante à dada por Cassels (Cassels, 1978) e por Rose (Rose, 1988); chegaremos ao mesmo resultado (as classes de formas com mesmo discriminante formam um grupo abeliano). A formulação de Gauss mostrou-se difícil de trabalhar, e em 1851 Dirichlet propôs uma nova visão de composição, mais simples, e usando as raízes da forma..
A idéia básica da composição de Dirichlet é primeiro transformar as duas formas em formas equivalentes onde a_1 e a_2 são co-primos.

No original,

> *234. Postquam haec de formis in classes genera et ordines distribuendis praemisimus, proprietatesque generales quae ex his distinctionibus statim defluunt explicauimus, ad aliud argumentum grauissimum transimus a nemine hucusque attactum, de formarum compositione.*

Gauss, Johann Carl Friedrich. **Disquisitiones Arithmeticae**. [*S. l.*], 1801.

[17] Johann Peter Gustav Lejeune Dirichlet. O tratado é

Dirichlet, Johann Peter Gustav Lejeune. **De formarum binariarum secundi gradus compositione**. [*S. l.: s. n.*], 1851. Reproduzido em Jour. fur Math., 47, 1854, 155-160; Werke, II, 1897, 105-114. Trad Francês, Jour, de Math., (2), 4, 1859, 389-398.

No que segue, tratamos das classes de equivalência de formas com um mesmo discriminante. Por exemplo, há três formas primitivas reduzidas com discriminante -44:

$$(1,0,11),(3,2,4),(3,-2,4).$$

Estas três formas são representantes de classes de equivalência. Por exemplo,

$$\begin{aligned}(1,0,11) &\sim (1,2,12)\\ (3,2,4) &\sim (4,-2,3)\end{aligned}$$

Mas a classe de $(1,0,11)$ é diferente da classe de $(3,2,4)$: basta perceber que 1 é representável por $f=(1,0,11)$, mas não por $g=(3,2,4)$.

$$f(1,0)=1(1)+0(1\cdot 0)+11(0)=1$$

Mas $g(x,y)=3x^2+2xy+4y^2$, que sempre será maior que 1.

Definição 11.17 (formas quadráticas concordantes)**.** *Duas formas primitivas* (a_1,b_1,c_1) *e* (a_2,b_2,c_2) *são* ***concordantes*** *se*[18] $a_1a_2\neq 0$, $b_1=b_2$ *e* $a_2\mid c_1$. ◀

É importante que, dadas duas classes de formas quadrática com o mesmo discriminante, sempre é possível encontrar duas formas, uma de cada classe, que são concordantes. Isso possibilitará falar de "composição de formas" como uma operação entre classes.
Também é fato relevante que se $\operatorname{mdc}(a_1,a_2)=1$ a restrição $a_2\mid c_1$ é desnecessária.

Teorema 11.17. *Sejam* f *e* g *formas primitivas com o mesmo discriminante* Δ*, pertencentes a classes diferentes. Então existem* F *e* G*, concordantes, tais que*

$$\begin{aligned}f &\sim F\\ g &\sim G.\end{aligned}$$

Definição 11.18 (composição de formas quadráticas e de classes de formas)**.** *Se as formas* $f=(a_1,b,c_1)$ *e* $g=(a_2,b,c_2)$ *tem o mesmo discriminante, então a* ***composição das formas*** f *e* g *é*

$$\begin{aligned}f*g &= (a_1a_2,b,c_2/a_1)\\ &= (a_1a_2,b,c_1/a_2).\end{aligned}$$

[18] A exigência $a_1a_2\neq 0$ pode parecer estranha inicialmente – porque não simplesmente dizer "a_1, a_2 não nulos"? Isso é feito porque estes conceitos podem ser usados também módulo p (mas isto não será feito neste texto).

De maneira semelhante, se C_1 *e* C_2 *são duas classes de formas com o mesmo discriminante,* $f_1 \in C_1$, $f_2 \in C_2$, *então a forma* $f_1 * f_2$ *pertence a uma classe* C_3, *que é denominada a* ***composição das classes*** C_1 *e* C_2, *denotada* $C_3 = C_1 * C_2$. ◀

A definição afirma que $c_2/a_1 = c_1/a_2$. Isto é facilmente verificável, escrevendo c em função de Δ. De fato, é comum, ao tratar de formas com o mesmo discriminante, escrever $(a, b, *)$ ou $(a, b, _)$, porque c será determinado por a, b, Δ.
As definições de formas "concordantes" e de composição podem ser apresentadas de formas ligeiramente diferentes na literatura[19].

Exemplo 11.11. *Seja* $\Delta = -120$. *Há quatro classes para este discriminante:*

$$(1, 0, 30)$$
$$(2, 0, 15)$$
$$(3, 0, 10)$$
$$(5, 0, 6)$$

A composição $(3, 0, 10) * (5, 0, 6)$ *é*

$$\begin{aligned}(3 \cdot 5, 0, 2) &= (15, 0, 2) \\ &\sim (2, 0, 15) \qquad \text{(redução da forma, (a,b,c) } \Rightarrow \text{(c,-b,a))}\end{aligned}$$

A composição $(2, 0, 15) * (3, 0, 10)$ *é*

$$\begin{aligned}(2 \cdot 3, 0, 15/3) &= (6, 0, 5) \\ &\sim (5, 0, 6) \qquad \text{(redução da forma, (a,b,c) } \Rightarrow \text{(c,-b,a))}\end{aligned}$$

A composição $(1, 0, 30) * (3, 0, 10)$ *é*

$$(1 \cdot 3, 0, 10/1) = (3, 0, 10),$$

e $(1, 0, 30)$ *é, portanto, neutro para composição.* ◀

Lema 11.3. *Se o discriminante de* f *e o de* g *são iguais a* Δ, *então o discriminante de* $f * g$ *também é* Δ.

[19] Por exemplo, duas formas (a_1, b_1, c_1) e (a_2, b_2, c_2) podem ser ditas "concordantes" em alguns textos quando

$$\operatorname{mdc}\left(a_1, a_2, \frac{b_1 + b_2}{2}\right) = 1.$$

Neste caso, a composição de formas é apresentada de maneira diferente:

$$(a_1, b_1, c_1) \underline{*} (a_2, b_2, c_2) = (a_1 a_2, B, *),$$

onde $B \equiv b_1 \pmod{a_1}$ e $B \equiv b_2 \pmod{a_2}$.

Lema 11.4. *Se* f *e* g *tem o mesmo discriminante e representam* 1*, então* $f \sim g$.

Lema 11.5. *Para a composição de classes, a identidade é a classe da forma principal (Definição 11.12*[20]*).*

Demonstração. A identidade é a classe de $(a, b, *)$ deve ser a classe de $(1, b, *)$, já que

$$(1, b, *)(a, b, *) = (a, b, *)$$

Mas $(1, b, *)$ representa 1, com valores $x = 1, y = 0$; e a forma principal também representa 1, com os mesmos valores. Portanto a forma principal da classe é equivalente a $(1, b, *)$, e esta classe é a identidade. □

Lema 11.6. *A inversa de uma forma* $f = (a, b, c)$ *é* $f^{-1} = (c, b, a)$.

Demonstração. Trivialmente, $(c, b, a) * (a, b, c) = (ac, b, 1)$, que representa 1, e portanto é equivalente à forma principal do discriminante. □

Teorema 11.18. *O conjunto de classes de equivalência de formas quadráticas binárias com discriminante* Δ*, com a operação de composição, é um grupo abeliano finito.*

Demonstração. Segue diretamente dos lemas e teoremas nesta seção, faltando apenas demonstrar que a composição é associativa e comutativa. □

Exemplo 11.12. *Seja* $\Delta = -63$*. Há cinco classes para este discriminante:*

$$(1, 1, 16)$$
$$(2, 1, 8)$$
$$(4, 1, 4)$$
$$(8, 1, 2)$$

A tabela de multiplicação do grupo é mostrada a seguir. Na tabela, (a, b, c) *é denotado somente por* a*, a fim de simplificar a apresentação.*

$*$	1	2	4	8
1	1	2	4	8
2	2	4	8	1
4	4	8	1	2
8	8	1	2	4

[20] **Definição 11.12:** A **forma principal** de um discriminante Δ é

$$\left(1, 0, \frac{-\Delta}{4}\right) \text{ se } \Delta \equiv 0,$$
$$\left(1, 1, \frac{-(\Delta - 1)}{4}\right) \text{ se } \Delta \equiv 1.$$

Nem todas as operações são imediatas. É um exercício interessante tentar chegar a todos os resultados – pode ser necessário reduzir formas, ou realizar a operação com formas equivalentes. Por exemplo, ao tentar diretamente calcular $(4,1,4) * (8,1,2)$*, nota-se que* $4 \nmid 8$ *(as formas não são concordantes), e para não chegar a forma resultante* $(32,1,1/2)$*, é necessário encontrar formas equivalentes concordantes ou, neste caso, simplesmente observar que*

$$\begin{aligned} f &= (8,1,2) * (4,1,4) \\ (8,1,2)^{-1} * f &= (4,1,4) \\ (2,1,8) * f &= (4,1,4) \\ (2,1,8) * (a,1,c) &= (4,1,4) \end{aligned}$$

onde

$$\begin{aligned} 2a &= 4 \\ 8/a &= c/2 \end{aligned}$$

Temos portanto $a = 2$*,* $c = 8$*, e*

$$f = (2,1,8).$$

Outros casos onde $c_i \nmid a_j$ *(e portanto as formas não são concordantes) podem ser resolvidos encontrando formas concordantes.* ◀

11.3 Formas quadráticas ternárias

Com três variáveis, as formas que estudamos são chamadas *formas quadráticas ternárias.*

Definição 11.19 (forma quadrática ternária (integral))**.** *Uma* ***forma quadrática ternária*** *é uma forma quadrática em três variáveis. Uma forma quadrática ternária é* ***integral*** *se todos os componentes de sua matriz são inteiros.* ◀

Para que uma forma quadrática ternária seja integral não basta que os coeficientes do polinômio sejam integrais; isso é requerido da *matriz* que representa a forma.

Exemplo 11.13. *A forma ternária representada pela matriz*

$$\begin{pmatrix} 2 & 1/2 & 0 \\ 1/2 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

não *é integral, porque* $a_{12} = a_{21} = 1/2$*, ainda que o polinômio que ela representa tenha coeficientes inteiros:*

$$\begin{aligned} f(x_1, x_2, x_3) &= \begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} \begin{pmatrix} 2 & 1/2 & 0 \\ 1/2 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \\ &= 2x_1^2 + x_2^2 + x_1x_2 + 2x_3^2. \end{aligned}$$

◀

Daqui adiante trataremos apenas de formas ternárias que são integrais.

Há dois Teoremas que apresentaremos sem demonstração, e que serão usados na demonstração do teorema dos três quadrados.

Teorema 11.19. *Toda forma quadrática ternária positiva definida integral com determinante um é equivalente a uma soma de três quadrados.*

Exemplo 11.14. *A forma quadrática representada pela matriz*

$$Q = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

é

$$f(x_1, x_2, x_3) = x_1^2 + 2x_2^2 + 2x_1x_2 + 5x_3^2$$

A matriz tem determinante um, portanto Q *é equivalente a uma matriz que representa soma de três quadrados: seja*

$$R = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Então

$$RQR^T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

que representa a forma $x_1^2 + x_2^2 + x_3^2$*.* ◀

Teorema 11.20. *Uma forma quadrática* $f(x_1, x_2, x_3)$ *é positiva definida se e somente se*

$$a_{11}, \quad \det f, \quad \det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

forem todos estritamente maiores que zero.

Exemplo 11.15. *A forma apresentada no Exemplo 11.14,*

$$Q = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

é positiva definida, porque

$$\begin{aligned} a_{11} &= 1 > 0 \\ \det Q &= 1 > 0 \\ \det \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} &= 2 - 1 = 1 > 0. \end{aligned}$$

◀

11.3.1 Aplicação: soma de três quadrados

Esta seção ilustra uma aplicação de formas quadráticas: a demonstração do Teorema dos três quadrados, de Gauss-Legendre. Esta demonstração depende de um Teorema de Dirichlet, cujo enunciado é bastante simples, mas (como mencionamos no início do livro) tem uma demonstração não trivial, e que apresentamos sem demonstração.

Teorema 11.21 (de Dirichlet)**.** *Sejam* $a, b \in \mathbb{Z}$*, com* $\operatorname{mdc}(a, m) = 1$*. Então Existem infinitos primos na sequência* $a, a + m, a + 2m, \ldots, a + rm, \ldots$*, com* $r \in \mathbb{N}$*.*

Enunciamos novamente o Teorema 10.7 (dos três quadrados, de Gauss-Legendre).

Teorema 11.22 (de Gauss-Legendre)**.** *Um inteiro positivo é representável como soma de três quadrados se e somente se não é da forma* $4^m(8k + 7)$*.*

Um sentido do teorema já foi demostrado no Capítulo 10 (que a soma de três quadrados precisa ser da forma dada). Demonstramos o outro sentido (que todo número dessa forma é soma de três quadrados) agora, usando formas quadráticas ternárias[21].

Demonstração. Inicialmente, suponha que $n = 4^k m$, e $4 \nmid m$. Então $m = x^a + y^2 + z^2$ é soma de tres quadrados. Mas neste caso,

$$n = 4m = (2^k x)^2 + (2^k y)^2 + (2^k z)^2$$

também é soma de tres quadrados. Podemos, portanto, presumir que $4 \nmid n$.

[21] Esta demonstração é bastante conhecida, e é essencialmente (com adaptações) a demonstração dada por Edmund Landau.

Landau, Edmund. **Elementary Number Theory**. New York, NY: Chelsea Publishing Company, 1958.

Também descartamos o caso $n = 8k+7$, portanto consideramos somente os casos $n = 1, 2, 3, 5, 6 \pmod 8$.

Construiremos uma forma quadrática ternária positiva definida, com determinante um, que represente n. Como, pelo Teorema[22] 11.19, toda forma quadrática positiva definida com determinante um é equivalente a uma soma de três quadrados, teremos provado que n é representável como soma de três quadrados.

A fim de simplificar a notação, denotaremos por B o determinante da submatriz de ordem 2 na matriz da forma,

$$B = \det \begin{pmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{pmatrix} = a_{11}a_{22} - a_{12}^2.$$

De acordo com o Teorema[23] 11.20, a forma ternária positiva definida que represente n, com determinante um, deverá ter

$$\begin{aligned} a_{11} &> 0 \\ B = a_{11}a_{22} - a_{12}^2 &> 0 \end{aligned}$$

Escolha $a_{13} = 1$, $a_{23} = 0$ e $a_{33} = n$. A forma será

$$f = \begin{pmatrix} a_{11} & a_{12} & 1 \\ a_{12} & 1_{22} & 0 \\ 1 & 0 & n \end{pmatrix}$$

e teremos

$$f(x_1, x_2, x_3) = a_{11}x_1^2 + 2a_{12}x_1x_2 + 2x_1x_3 + a_{22}x_2^2 + nx_3^2,$$

de maneira que $f(0, 0, 1) = n$ – e a forma representará n.

Precisamos então determinar os três valores, a_{11}, a_{12} e a_{22} – e quando o fizermos a demonstração estará pronta.

[22] **Teorema 11.19:** Toda forma quadrática ternária positiva definida integral com determinante um é equivalente a uma soma de três quadrados.

[23] **Teorema 11.20:** Uma forma quadrática $f(x_1, x_2, x_3)$ é positiva definida se e somente se

$$a_{11}, \quad \det f, \quad \det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

forem todos estritamente maiores que zero.

Observamos que o determinante de f deve ser 1.

$$\begin{aligned}\det\begin{pmatrix} a_{11} & a_{12} & 1 \\ a_{12} & a_{22} & 0 \\ 1 & 0 & n \end{pmatrix} &= a_{11}a_{22}n - a_{22} - a_{12}a_{12}n \\ &= Bn - a_{22} \\ &= 1\end{aligned}$$

As condições que precisamos satisfazer são

$$\begin{aligned} a_{11} &> 0 \\ B = a_{11}a_{22} - a_{12}^2 &> 0 \\ Bn - a_{22} &= 1 \end{aligned}$$

Como 1 claramente soma de três quadrados, presumimos adiante que $n > 1$. Se $B > 0$ e $n > 1$,

$$a_{22} = Bn - 1 > b - 1 \geq 0.$$

Mas também teremos

$$a_{11}a_{22} = B + a_{12}^2 > 0$$

Como o lado direito é positivo e $a_{22} > 0$, então necessariamente $a_{11} > 0$. Podemos eliminar a condição $a_{11} > 0$, porque ela será automaticamente satisfeita. Nos restam as condições

$$\begin{aligned} B = a_{11}a_{22} - a_{12}^2 &> 0 \\ Bn - 1 &= a_{22} \end{aligned}$$

Então B deve ser tal que

$$a_{11} = \frac{B + a_{12}^2}{a_{22}}, \tag{11.1}$$

sendo que $a_{11} \in \mathbb{Z}$. Mas isto é o mesmo que dizer que queremos $B > 0$, com

$$\begin{aligned} b + a_{12}^2 &\equiv 0 \pmod{a_{22}} \\ -b &\equiv +a_{12}^2 0 \pmod{a_{22}} \\ -b &\equiv +a_{12}^2 0 \pmod{Bn - 1} \end{aligned}$$

Os passos para completar a matriz da forma f portanto são:

i) Escolher $a_{22} = Bn - 1$;

ii) Escolher a_{12} como a raiz quadrada de $-B$ módulo $Bn - 1$ (e para isto precisamos que $-B$ ecolhido no passo (i) seja resíduo quadrático módulo $Bn - 1$);

iii) Escolher a_{11} de acordo com a equação 11.1.

Lembramos que a demonstração deve valer para $n \equiv 1, 2, 3, 5, 6 \pmod 8$. Separamos em dois casos – n par e n ímpar.
Se n é par, então $n \equiv 2 \pmod 8$ ou $n \equiv 6 \pmod 8$. Queremos um primo $p = Bn - 1$ tal que

$$\left(\frac{-B}{p}\right) = +1.$$

Seja $d = \mathrm{mdc}\,(4n, n\text{-}1)$. Então $d \mid 4n - 4(n-1) = 4$, e necessariamente d deve ser $1, 2$ ou 4. Pelo Teorema[24] 11.21 (de Dirichlet), existe algum $t > 0$ tal que

$$p = 4nt + n - 1 = (4t + 1)n - 1$$

é primo.
Escolha $B = 4t + 1 > 0$ e então $p = Bn - 1$. Agora temos $B \equiv 1 \pmod 4$ e $p \equiv n - 1 \equiv 1 \pmod 4$, e

$$\begin{aligned}
\left(\frac{-B}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{B}{p}\right) \\
&= \left(\frac{B}{p}\right) && (p = 4k + 1,\ \text{Lema}[25]\ 9.1) \\
&= \left(\frac{p}{B}\right) && (p = 4k + 1,\ \text{recip. quad.}) \\
&= \left(\frac{Bn - 1}{B}\right) \\
&= \left(\frac{-1}{B}\right) \\
&= +1. && (B = 4k + 1,\ \text{Lema } 9.1)
\end{aligned}$$

Agora, se n é ímpar, então n deve ser $1, 3$ ou 5 módulo 8. Seja

$$c = \begin{cases} 1 & n \equiv 3 \pmod 8, \\ 3 & n \equiv 1, 5 \pmod 8. \end{cases}$$

Desta forma teremos sempre $cn \equiv 3 \pmod 4$, e $(cn - 1)/2$ é ímpar. Seja

[24] **Teorema 11.21 (de Dirichlet):** Sejam $a, b \in \mathbb{Z}$, com $\mathrm{mdc}\,(a, m) = 1$. Então Existem infinitos primos na sequência $a, a + m, a + 2m, \ldots, a + rm, \ldots$, com $r \in \mathbb{N}$.
Veja que isto significa que, dados $4n$ e $n - 1$, existem infinitos números primos da forma $n - 1 + (4n)t$.

[25] **Lema 9.1:** Se p é primo ímpar,

$$\left(\frac{-1}{p}\right) = \begin{cases} +1 & \text{se } p = 4k + 1, \\ -1 & \text{se } p = 4k + 3. \end{cases}$$

$h = \mathrm{mdc}\,(4n, (cn\text{-}1)/2))$. Temos dois casos:

I) $c = 1$: então $h \mid 4n - 8((n-1)/2) = 4$,

II) $c = 3$: então $h \mid 4(4n) - 8((3n-1)/2) = 4$.

De qualquer maneira, $h \mid 4$, portanto $h = 1$ porque $(cn-1)/2$ é ímpar. Novamente usamos o Teorema de Dirichlet para determinar $t' > 0$ tal que

$$p = 4nt' + \frac{cn-1}{2} = \frac{(8t'+c)n-1}{2}$$

é primo.

Seja $B = 8t' + c$. Como $B > 0$, então $2p = Bn - 1$, precisamos mostrar que B é quadrado módulo $2p$. Consideramos três casos:

i) $n \equiv 1 \pmod 8$. Então $B \equiv 3 \pmod 8$ e $p \equiv 1 \pmod 4$

ii) $n \equiv 3 \pmod 8$. Então $B \equiv 1 \pmod 8$ e $p \equiv 1 \pmod 4$

iii) $n \equiv 5 \pmod 8$. Então $B \equiv 3 \pmod 8$ e $p \equiv 3 \pmod 4$

Nos três casos,

$$\left(\frac{-2}{B}\right) = \left(\frac{-1}{B}\right)\left(\frac{2}{B}\right) = +1, \tag{11.2}$$

onde usamos o Corolário[26] 9.2. Também temos

$$\left(\frac{-B}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{B}{p}\right) = \left(\frac{p}{B}\right). \tag{11.3}$$

A última passagem se justifica porque (i) se $p \equiv 1 \pmod 4$, então $(-1/p)\,(B/p) = (1)(B/p) = (p/B)$; e se $p \equiv 3 \pmod 4$ então $B \equiv 3 \pmod 4$ também, e $(-1/p)\,(B/p) = (-1)(B/p) = (-1)(-1)(p/B)$.

[26] **Corolário 9.2:** Se $n \in \mathbb{Z}$ é ímpar, então

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}.$$

Juntando tudo,

$$\begin{aligned}
\left(\frac{-B}{p}\right) &= \left(\frac{p}{B}\right) && \text{(por 11.3)}\\
&= \left(\frac{p}{B}\right)\left(\frac{-2}{B}\right) && \text{(por 11.2, } (-2/B) = +1\text{)}\\
&= \left(\frac{-2p}{B}\right)\\
&= \left(\frac{1-Bn}{B}\right) && (2p = Bn - 1)\\
&= \left(\frac{1}{B}\right)\\
&= +1. && \text{(1 sempre é quadrado)}
\end{aligned}$$

Conseguimos um núemro $-B$ que é resíduo quadrático módulo p – mas ainda não é suficiente.
Escolha x' tal que $(x')^2 \equiv -B \pmod{p}$. Determine

$$x = \begin{cases} x' & x' \text{ é ímpar} \\ x' + p & x' \text{ é par} \end{cases}$$

Nos dois casos, x será ímpar, e $x^2 + B$ será par, e teremos

$$x \equiv x' \pmod{p}.$$

Finalmente,

$$\begin{aligned}
r^2 + b &\equiv 0 \pmod{p}\\
r^2 + b &\equiv 0 \pmod{2}
\end{aligned}$$

Como 2 e p são coprimos, temos finalmente

$$\begin{aligned}
r^2 + b &\equiv 0 \pmod{2p}\\
r^2 &\equiv -b \pmod{2p},
\end{aligned}$$

completando a demonstração. □

Exercícios

Ex. 296 — Prove que a seguinte definição é equivalente à dada no texto.

Definição 11.20 (forma quadrática)**.** *Seja V um espaço vetorial de dimensão finita sobre um corpo K com característica diferente de 2 (ou seja,*

$1+1 \neq 0$ *em* K*). Uma função* $f : V \times V \to K$ *é uma* ***forma quadrática*** *se*

- $\forall\, k \in K$, $v \in V$, $f(kv) = k^2 f(v)$
- *a função* $b(v,w) = f(v+w) - f(v) - f(w)$ *é uma forma bilinear.* ◀

Ex. 297 — (Fácil) Seja $f = ax^2 + bxy + cy^2$ uma forma quadrática binária. Mostre que $b \equiv \Delta(f) \pmod 2$.

Ex. 298 — Quais das formas são equivalentes? $x^2 + 2xy + 4y^2$, $x^2 - 2xy - 21y^2$, $-2x^2 - y^2$, $2x^2 + 4xy + 3y^2$.

Ex. 299 — Seja $\Delta \in \mathbb{Z}$ um quadrado perfeito. Mostre que existe um forma quadrática binária $ax^2 + bxy + cy^2$ com discriminante Δ e $a = 0$.

Ex. 300 — Demonstramos que se f e g são equivalentes (existe matriz unimodular U, $F = U^T G U$). Agora tente seguir os passos na direção da recíproca:
Suponha que para todo $n \in \mathbb{Z}$, f representa n se e somente se g também representa n. Então:

i) Existe uma matriz que transforma G em F?

ii) Com determinante ± 1?

iii) E integral?

Ex. 301 — Seja f uma forma quadrática binária com discriminante negativo e $n \in \mathbb{Z}$. Mostre como resolver a equação diofantina $f(x,y) = n$.

Ex. 302 — Seja f uma forma quadrática binária com discriminante negativo e $n \in \mathbb{R}$. Mostre que a quantidade de soluções para $f(x,y) = n$ é finita.

Ex. 303 — Prove que todo discriminante pode ser escrito de forma única como $k^2\Delta$. onde Δ é discriminante fundamental.

Ex. 304 — Prove que Δ é discriminante fundamental se e somente se

i) Δ não é divisível pelo quadrado de um primo ímpar; e

ii) Δ é da forma $16k + 8$ ou da forma $16k + 12$.

Ex. 305 — Um discriminananante fundamental $\Delta \in \mathbb{Z}$ é **primo** se é divisível por exatamente um inteiro primo. Prove que se $\Delta \in \mathbb{Z}$ é um discriminante fundamental, então Δ pode ser escrito de forma única (a não ser por ordem) como produto de discriminantes primos.

Ex. 306 — Demonstre: sejam $n, \Delta \in \mathbb{Z}$, com $n > 3$ e $\operatorname{mdc}(n, \Delta) = 1$. Então n tem representação própria por forma primitiva com discriminante Δ se e somente se Δ é resíduo quadrático módulo n.

Ex. 307 — Encontre uma definição sucinta para forma quadrática definida reduzida. A definição deve valer para formas positivas e negativas, sem a necessidade de separar explicitamente estes dois casos.

Ex. 308 — Demonstre o final do Teorema 11.15.

Ex. 309 — Demonstre o Corolário 11.4.

Ex. 310 — Prove que um automorfismo de uma forma quadrática binária (a, b, c) sempre é da forma

$$\begin{pmatrix} \frac{j - bk}{2} & ak \\ -ck & \frac{j + bk}{2} \end{pmatrix}$$

onde $j, k \in \mathbb{Z}$ são soluções da equação de Pell $j^2 - \Delta k^2 = 4$.

Ex. 311 — Prove que os automorfismos de uma forma quadrática binária formam um grupo.

Ex. 312 — Prove que os grupos de automorfismos das formas primitivas com um mesmo determinante são isomorfos.

Ex. 313 — Prove que toda forma definida com determinante 1 é equivalente à forma $x^2 + y^2$.

Ex. 314 — Prove que todo primo da forma $4k + 1$ pode ser escrito como soma de dois quadrados, usando o Teorema 11.10. (Ou seja, apresente uma demonstração alternativa para o Teorema 10.2).

Ex. 315 — Prove que se o determinante de uma forma quadrática binária f é quadrado perfeito, então existem $x, y \in \{0, 1\}$, pelo menos um deles diferentes de zero, tais que $f(x, y) = 0$.

Ex. 316 — Termine a demonstração do Teorema 11.16.

Capítulo 12

Formas Modulares, Grupo Modular

Este Capítulo é um esboço

12.1 O grupo modular

Uma *transformação linear fracionária* é uma função $f : \mathbb{C} \to \mathbb{C}$, da forma

$$f(z) = \frac{az + b}{cz + d},$$

Representamos transformações como matrizes:

$$f = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Se tivermos f como dada acima, e definirmos uma outra transformação

$$g(z) = \frac{\alpha z + \beta}{\gamma z + \delta},$$

então a composição de f e g será

$$f(g(z)) = \frac{(b\gamma + a\alpha)z + b\delta + a\beta}{(d\gamma + c\alpha)z + d\delta + c\beta}.$$

É conveniente que a multiplicação de matrizes pode ser usada para representar a composição de transforamções lineares fracionárias. Se f e g são

da forma já dada, e F e G são suas matrizes, então

$$FG = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} b\gamma + a\alpha & b\delta + a\beta \\ d\gamma + c\alpha & d\delta + c\beta \end{pmatrix}$$

representa a composição de f com g.
O *grupo linear geral* de grau n, denotado $GL(n, F)$, é o grupo de matrizes invertíveis $n \times n$ sobre o corpo F, com a operação de multiplicação de matrizes. O *grupo linear especial* $SL(n, F)$ é o subgrupo de $GL(n, F)$ contendo apenas as matrizes com determinante $+1$.
O grupo que representa as transformações lineares fracionárias que nos interessam é um subgrupo de $SL(n, F)$ chamado de *grupo modular*, ou *grupo linear especial projetivo*. Em $SL(n, F)$, as matrizes A e $-A$ são tratadas como o mesmo elemento.

Definição 12.1 (grupo modular / grupo linear especial projetivo $PSL(2, \mathbb{Z})$)**.** *As matrizes 2×2 com elementos integrais e determinante 1, usando a operação usual de multiplicação de matrizes, formam o* grupo modular*, também chamado de* grupo linear especial projetivo*. Equivalentemente, as transformações da forma*

$$T(z) = \frac{az + b}{cz + d},$$

com $a, b, c, d \in \mathbb{Z}$, $ad - bc = 1$, e usando a operação de composição de funções, formam o grupo modular. Este grupo é denotado por $PSL(2, \mathbb{Z})$, ou por Γ. ◀

Como exemplo,

$$M = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix} \in \Gamma,$$

porque todos os $m_{i,}$ são inteiros, e $\det M = 1$.

Teorema 12.1. *O grupo Γ é gerado pelas transformações $S(z) = -z^{-1}$ e $T(z) = z + 1$, ou seja,*

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

já definidos no Lema 11.1 do Capítulo 11 (página 308)[1]*.*

Demonstração. O efeito das matrizes S e T é simples: S realiza troca de linhas, e como o determinante deve se manter um, S também realiza a troca

[1] **Lema 11.1:** Dados $a, b, c, k \in \mathbb{Z}$, então

i) $(a, b, c) \sim (c, -b, -a)$, e

ii) $(a, b, c) \sim (a, b + 2ka, ak^2 + bk + c)$.

do sinal do determinante; T soma a segunda linha à primeira.

$$T\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}, \quad S\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}$$

Para mostrar que qualquer matriz de Γ é produto das matrizes T e S, começamos com uma matriz qualquer de Γ:

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Suponha que c seja zero. Como $\det M = 1$ e os elementos são todos inteiros, então a diagonal só pode ser $a = d = \pm 1$. Mas isto significa que M é T^n, para algum n, já que

$$T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

Suponha, então, que $c > 0$. Suponha também que $|a| > |c|$ (se não for, pode-se usar S para trocar as linhas).
Agora faremos a divisão de a por c: $a = qc + r$, com $0 \leq r < |c|$. Isto pode ser realizado multiplicando T^{-q}:

$$T^{-q}M = \begin{pmatrix} a - qc & b - qd \\ c & d \end{pmatrix}.$$

Se $a - qc$ for zero, paramos. Senão, usamos S para trocar as linhas e recomeçamos. Este é essencialmente o algoritmo de Euclides para cálculo de MDC, e eventualmente o valor na posição $(1,1)$ da matriz será zero, e usaremos S uma última vez para trocar as linhas para que a posição $(2,1)$ passe a ser zero. Como o determinante da matriz não foi alterado (porque só usamos T e S), a diagonal será composta por uns, com o mesmo sinal, e portanto será igual a T^k, para algum k. □

Corolário 12.1. *Toda matriz $M \in \Gamma$ pode ser escrita como*

$$M = T^{k_1} S T^{k_2} S \cdots T^{k_n}.$$

É relevante também que $S^2 = (ST)^3 = I$.
Exploramos a seguir a ação do grupo modular no meio-plano superior.

Definição 12.2 (meio-plano superior)**.** *Denotamos por $\mathbb{H}$ o* meio plano superior*, que no plano complexo contém os números com parte imaginária positiva,*

$$\mathbb{H} = \{a + bi \,:\, a, b \in \mathbb{R}, b > 0\}$$ ◀

Definição 12.3 (pontos equivalentes em $\mathbb{H}$)**.** *Dois pontos $z, z' \in \mathbb{H}$ são equivalentes quando existe $g \in \Gamma$ tal que $g(z) = z'$. Denotamos $z \sim z'$.* ◀

Definição 12.4 (região fundamental)**.** *Dado um grupo de transformações no plano, a* região fundamental *(também chamada de* "domínio fundamental"*) do grupo é uma região do plano que não contém dois pontos equivalentes, mas contém pontos representando todas as classes de equivalência.* ◀

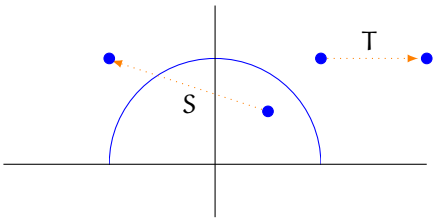
Por exemplo, as duas transformações $f(x,y) = (x+1, y)$, e $g(x,y) = (x, y+2)$ geram um grupo de transformações: o grupo contendo as transformações

$$\{h(x,y) = (ax, 2by) \ : \ a, b \in \mathbb{Z}\},$$

e a operação de composição de funções. Uma região fundamental desse grupo é o retângulo com vértices $(0,0)$, $(1,0)$, $(1,2)$, $(0,2)$.
Há algumas observações importantes sobre o efeito de S e T em $\mathbb{H}$.
A transformação S leva a parte imaginária de seu argumento

- de dentro para fora do círculo unitário, se $N(z) < 1$;
- de fora para dentro do círculo unitário, se $N(z) > 1$;
- da borda para para algum outro ponto também na borda do círculo unitário, se $N(z) = 1$, porque $S(z)$ deverá, neste caso, ter também norma um.

A interpretação geométrica: $1/z = \bar{z}/N(z)$, ou seja, inverter um complexo é realizar uma reflexão pelo eixo das abscissas, e mudar a magnitude do vetor. Logo, $-1/z$ realiza uma reflexão pelo eixo das ordenadas e divide a magnitude por $N(z)$.
A transformação T realiza uma translação, não alterando a parte imaginária do número.



A seguir identificaremos um domínio fundamental para Γ.

Lema 12.1. *O ponto* $\rho = (-1 + i\sqrt{3})/2$ *é mapeado em si mesmo somente pelas transformações*

$$z' = z, \quad z' = -\frac{1}{z+1}, \quad z' = -1 - \frac{1}{z},$$

ou seja, a identidade, ST *e* $T^{-1}S$*.*

O ponto i *é mapeado em si mesmo somente pela identidade e por* S*,*

$$z' = z, \quad z' = -\frac{1}{z},$$

Qualquer outro ponto em R *é mapeado em si mesmo apenas pela identidade.*

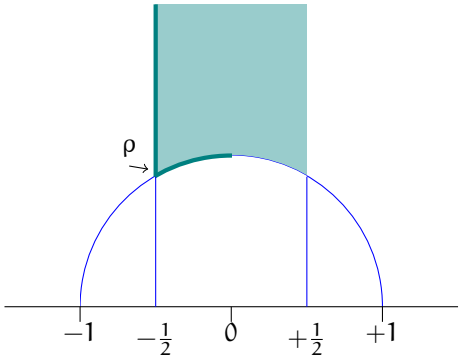
As transformações ST e $T^{-1}S$ mapeiam ρ nele mesmo porque S tem o mesmo efeito que T em ρ. Em i, S claramente não tem efeito, porque i é unidade.

Teorema 12.2. *Seja*

$$R = \left\{ z \in \mathbb{H} \,:\, \mathrm{Re}(z) \in \left[-\frac{1}{2}, +\frac{1}{2}\right), N(z) > 1 \right\}$$
$$\bigcup \left\{ z \in \mathbb{H} \,:\, \mathrm{Re}(z) \in \left[-\frac{1}{2}, 0\right), N(z) = 1 \right\}$$

Então R *é região fundamental de* Γ*.*

A figura a seguir ilustra a região R, e o ponto $\rho = (-1 + \sqrt{3})/2$. Note que a região é fechada no segundo quadrante, e aberta no primeiro. Isto é importante, porque de outra forma, teríamos dois pontos equivalentes na região fundamental: por exemplo, se $x = i - 1/2$ e $y = i + 1/2$, então ambos estariam em R e $y = T(x)$.



Demonstração. Demonstraremos que (i) para todo $z \in \mathbb{H}$, $z = f(z')$, com $f \in \Gamma$; e (ii) que se $z, z' \in R$, e existe $f \in \Gamma$, com $z = f(z')$, então $z = z'$.
(i) Passo um: seja $z \in \mathbb{H}$, e suponha que $N(z) > 1$. Então existe alguma n-ésima potência de T tal que $T^n(z)$ tem a parte real em $[-1/2, +1/2)$. Se, além disso, $T^n(z)$ está em R, terminamos. Senão, é porque a translação levou de fora para dentro do círculo unitário, mas não para dentro de R. Então a norma é menor que 1, e usamos o passo dois.
Passo dois: se $N(z) < 1$, realizamos uma inversão com S. Esta inversão aumentará a parte imaginária de z. Se o resultado é um ponto em R, terminamos. Senão, voltamos ao passo um.

Estes passos (T^k seguido de S) podem ter que ser repetidos um número finito de vezes, porque eventualmente a parte imaginária será maior que 1, e uma translação será suficiente para chegar a R.

Como T e S são bijeções, todo $z \in \mathbb{H}$ é igual a $f(z')$, para algum $f \in \Gamma$ e algum $z' \in R$.

(ii) Suponha que $g \in \Gamma$, e $z \in R$. Agora, suponha que $g(z) = z'$. Suponha também, sem perda de generalidade, que $\mathrm{Im}(gz) \geq \mathrm{Im}(z)$, ou seja, que z' está acima de z no meio-plano $\mathbb{H}$. Mas para que isto seja verdade,

$$|cz + d| \leq 1.$$

Como $|z| > 0$, então necessariamente $|c| \leq 1$. Uma vez que $c \in \mathbb{Z}$, então

$$c \in \{-1, 0, +1\}.$$

Se $c = -1$, podemos trocar g por $-g = \left(\begin{smallmatrix} -a & -b \\ -c & -d \end{smallmatrix}\right)$, e teremos a mesma transformação com $c = +1$, por isso tratamos apenas dos casos $c = 0$ e $c = +1$.

Se $c = 0$, então

$$g(z) = \frac{az + b}{cz + d} = \frac{az + b}{d}$$

Mas $ad - bc = 1$, e como $c = 0$, temos $ad = 1$, com $a, d \in \mathbb{Z}$. Assim, $a, d = \pm 1$. Com isso teremos

$$g(z) = z + b,$$

e $g(z) = T^n(z)$. Mas como a translação não pode mudar a parte imaginária de um número, e a largura da região que escolhemos como domínio fundamental é 1, então $b = 0$ e g é a identidade, logo $z = z'$.

Se $c = +1$, então há duas possibilidades: (i) $d = 0$, ou (ii) $d = 1$ e $z = \rho$. No primeiro caso, com $d = 0$ e $c = 1$, temos $|cz + d| \leq 1$, logo $|z + 1| \leq 1$. Mas isso implica que $|z| = 1$. Como $ad - bc = 1$, então $-bc = 1$, e $b = -c = -1$. A transformação teria que ser, portanto,

$$g(z) = \frac{az + b}{cz + d} = a - \frac{1}{z},$$

ou seja, $T(S(z))$. Mas, como a parte imaginária de z estava em R, era maior que um. E esta transformação muda a parte imaginária para algo menor que um (porque aplica S, e em seguida T), e portanto z e $g(z)$ não podem estar ambos em R.

No segundo caso, $c = +1$, $z = \rho$, $d = 1$,

$$g(z) = \frac{az + b}{z + 1}$$

Mas $ad - bc = 1$, portanto $a - b = 1$, e

$$\begin{aligned} g(z) &= \frac{az + (a-1)}{z+1} \\ &= a - \frac{1}{\rho + 1}, \end{aligned}$$

novamente uma inversão seguida de translação. Mas como $N(\rho) = 1$, sua parte imagniária não é modificada por g, e a transformação é uma translação – novamente, temos que necessariamente g é a identidade, e $g(\rho) = \rho$. □

12.2 Formas Quadráticas Binárias Definidas

Se uma forma quadrática (a, b, c) é positiva definida tem discriminante menor que zero, e por isso as raízes da equação $ax^2 + bx + c = 0$ são dois números complexos, com parte imaginária diferente de zero. Isso nos permite usar uma definição bastante simples para forma reduzida.

Sejam $z, \overline{z}$ as duas raízes da equação. Uma delas tem a parte imaginária positiva, e portanto está no meio-plano superior. Sem perda de generalidade, suponha que esta seja z. Tome o representante da classe de equivalência de z na região fundamental de Γ.

Teorema 12.3. *Se uma forma quadrática $ax^2 + bxy + cy^2$ definida positiva está na forma reduzida – ou seja,*

$$-a < b \leq a < c \quad \text{ou} \quad 0 \leq b \leq a = c,$$

então uma de suas duas raízes complexas está no domínio fundamental de Γ.

Demonstração. Seja z a raiz de $ax^2 + bx + c$ que está em $\mathbb{H}$. Separamos as partes real e imaginária de z

$$\begin{aligned} z &= \frac{-b + \sqrt{\Delta}}{2a} \\ &= \frac{-b}{2a} + \frac{\sqrt{\Delta}}{2a} \\ &= \frac{-b}{2a} + i\frac{\sqrt{-\Delta}}{2a} \end{aligned}$$

A norma de z é

$$\begin{aligned} N(z) &= \frac{b^2}{4a^2} + \frac{-\Delta}{4a^2} \\ &= \frac{b^2 - b^2 + 4ac}{4a^2} \\ &= \frac{c}{a}. \end{aligned}$$

Desta forma, para que $z \in R$, é necessário que a parte real esteja em $[-1/2, +1/2)$,

$$\begin{aligned} -\frac{1}{2} \leq \frac{-b}{2a} &< \frac{1}{2} \\ -a \leq -b &< a \\ a \geq b &> -a, \end{aligned}$$

e que a norma seja > 1 quando a parte real é positiva, e ≥ 1 quando a parte real é ≤ 0. No primeiro caso,$c/a > 1$ implica imediatamente que $c > a$. No segundo, temos $-b/2a > 0$ e $c/a = 1$, o que implica que $b \geq 0$ e $c = a$. Combinando as possibilidades, concluímos que uma forma definida positiva tem representante no domínio fundamental de Γ se

$$-a < b \leq a < c \quad \text{ou} \quad 0 \leq b \leq a = c,$$

conforme o enunciado. □

Na demonstração do Teorema 12.2[2], que afirma que R é domínio fundamental de Γ, há um algoritmo para trazer um ponto qualquer ed $\mathbb{H}$ para R. O mesmo algoritmo pode ser usado para transformar uma forma em outra equivalente, com raiz dentro de R. Basta aplicar as transformações na matriz da forma, ao invés de aplicá-las nos pontos (a aplicação das transformações S e T^k em uma matriz F é efetuada por $S^T F S$ e $(T^K)^T F T^K$). Este algoritmo é o mesmo apresentado no estudo das formas quadráticas reduzidas no Capítulo 11.

[2]**Teorema 12.2:** Seja

$$\begin{aligned} R = &\left\{ z \in \mathbb{H} \,:\, \mathrm{Re}(z) \in \left[-\frac{1}{2}, +\frac{1}{2}\right), N(z) > 1 \right\} \\ &\bigcup \left\{ z \in \mathbb{H} \,:\, \mathrm{Re}(z) \in \left[-\frac{1}{2}, 0\right), N(z) = 1 \right\} \end{aligned}$$

Então R é região fundamental de Γ.

12.3 Formas quadráticas indefinidas

Exercícios

Ex. 317 — Prove que o grupo Γ também pode ser gerado por

$$t(z) = z + 1$$
$$u(z) = \frac{z}{z+1}$$

Ex. 318 — Prove que o grupo Γ pode ser gerado por duas transformações de ordem finita no grupo (a transformação T, que usamos no gerador de Γ, não tem ordem finita!)

Ex. 319 — Encontre um domínio fundamental para Γ que contenha somente números com norma menor ou igual a um. Depois, formule uma definição alternativa de forma quadrática positiva definida reduzida usando esta região como referencia, e não a região R definida neste texto.

Ex. 320 — Seja n o produto de k primos da forma $8k+1$ ou $8k+3$. Prove que há 2^{k+1} representações próprias de n na forma $x^2 + 2y$, com $x, y > 0$.

Ex. 321 — Fixe $n \in \mathbb{Z}$, tal que $1 < n < 5$. Sejam

- Γ_1 o *grupo* gerado por $s(z) = -z^{-1}$ e $u(z) = z + \sqrt{n}$.
- Γ_2 o *conjunto* de todas as transformações lineares fracionárias das formas

$$q(z) = \frac{az + b\sqrt{n}}{c\sqrt{n} + d}, \quad ad - nbc = 1$$
$$r(z) = \frac{a\sqrt{n}z + b}{cz + d\sqrt{n}}, \quad adn - bc = 1,$$

  com $a, b, c, d \in \mathbb{Z}$.

Prove que Γ_2 é grupo, e que $\Gamma_2 = \Gamma_1$. Identifique um domínio fundamental para Γ_1, e prove que de fato é domínio fundamental. Se $\Gamma_2 \neq \Gamma_1$, faça o mesmo para Γ_2.

Capítulo 13

Corpos Quadráticos

Os números representados por frações contínuas infinitas e não periódicas (os exemplos usuais são e, π, ϕ, $\sqrt{2}$) não pertencem ao corpo dos racionais. Para incluí-los, e ainda assim obter um corpo, constrói-se um novo corpo, $\mathbb{R}$, que contém o corpo $\mathbb{Q}$. Isso é desenvolvido na Seção 15.5, usando frações contínuas, embora possa ser feito de diversas maneiras. Semelhantemente, percebendo que $x^2 = -1$ não tem solução em $\mathbb{R}$, criamos um outro corpo, $\mathbb{C}$, que contém $\mathbb{R}$, e onde postulamos que existe um elemento $i = \sqrt{-1}$.

13.1 Extensões de Corpos

Dizemos que $\mathbb{R}$ é uma *extensão* do corpo $\mathbb{Q}$, e que $\mathbb{C}$ é uma extensão de $\mathbb{R}$.

Definição 13.1 (extensão de corpo)**.** *Se E e F são corpos, e $F \subset E$, então E é uma **extensão** de F, o que denotamos por E/F a **extensão de** E **sobre** F.* ◀

Exemplo 13.1. *Os corpo dos reais são extensão do corpo dos racionais; o corpo dos complexos é extensão do corpo dos reais.* ◀

Exemplo 13.2. *$\mathbb{Z}_2$ é um corpo, contendo os elementos 0 e 1, e onde as operações são as usuais, mas módulo dois. É usual denotar $\mathrm{GF}(2)$ ao invés de $\mathbb{Z}_2$. Podemos construir um corpo com quatro elementos, que é uma extensão de $\mathrm{GF}(2)$. O conjnuto de polinômios*

$$\mathrm{GF}(4) = \{0, 1, x, x + 1\},$$

quando dotado de soma e multiplicação módulo $x^2 + x + 1$, é um corpo. Como $\mathrm{GF}(2) \subset \mathrm{GF}(4)$, então esta é uma extensão de $\mathrm{GF}(2)$. ◀

Cada número complexo pode ser descrito por dois reais, e é fácil verificar que as operações de soma e multiplicação fazem de $\mathbb{C}$ é um espaço vetorial sobre $\mathbb{R}$; uma possível base para este espaço é $\{1, i\}$. Isso vale também para

qualquer extensão de corpos: $\mathbb{R}$ é também um espaço vetorial sobre $\mathbb{Q}$, com dimensão infinita.

Teorema 13.1. *Se* E *é extensão de um corpo* F*, então* E *é um espaço vetorial sobre* F*.*

Demonstração. A operação de soma em E define um grupo comutativo, portanto já temos comutatividade, associatividade, neutro e inverso para soma, além de estar claro que a operação é fechada em E.
A multiplicação de $x \in F$ por $y \in E$ resulta em elemento de E (porque $F \subset E$, e portanto $x, y \in E$). Além disso, a multiplicação é associativa e distributiva (porque E é um corpo).
Há neutro para multiplicação: como $F \subset E$, e o neutro deve ser único, o mesmo elemento neutro em F é o neutro em E. □

Definição 13.2 (grau de extensão de corpo; extensão finita)**.** *O* ***grau da extensão*** E ***sobre*** F*, denotado* $[E : F]$*, é a dimensão de* E *como espaço vetorial sobre* F*. Quando* $[E : F]$ *é finito, dizemos que* E *é uma extensão finita de* F*.* ◀

Exemplo 13.3. $[\mathbb{C} : \mathbb{R}] = 2$*, porque* $\mathbb{C}$ *é espaço de dimensão dois sobre* $\mathbb{R}$*.* ◀

Exemplo 13.4. $\mathrm{GF}(4)$ *é espaço vetorial sobre* $\mathrm{GF}(2)$*, onde a base é* $B = \{1, x\}$*. Os elementos de* $\mathrm{GF}(4)$ *são combinações lineares dessa base, onde os coeficientes estão em* $\mathrm{GF}(2)$*:*

$$\begin{aligned} (\alpha)(\beta) &= \cdots && (\alpha\in\mathrm{GF}(2),\ \beta\in B)\\ (1)(0) &= 0\\ (1)(1) &= 1\\ (1)(x) &= x\\ (1)(x) + (1)(1) &= x + 1. \end{aligned}$$

Em todos os casos, o resultado é módulo $x^2 + x + 1$*.*
Como os $\mathrm{GF}(4)$ *é espaço vetorial sobre* $\mathrm{GF}(2)$*, com base* $\{1, x\}$*, de tamanho dois, então* $[\mathrm{GF}(4) : \mathrm{GF}(2)] = 2$*.* ◀

Teorema 13.2. *Se* E *é extensão de* F*, e* F *é extensão de* K*, então*

$$[E : K] = [E : F][F : K].$$

Exemplo 13.5. $\mathrm{GF}(8)$ *é o corpo com os elementos*

$$\begin{aligned} &0, 1, x, x + 1,\\ &x^2, x^2 + 1, x^2 + x, x^2 + x + 1 \end{aligned}$$

Este corpo é uma extensão de $\mathrm{GF}(4)$*, com grau* 2 *(ou seja,* $[\mathrm{GF}(8) : \mathrm{GF}(4)] = 2$*: cada elemento de* $\mathrm{GF}(8)$ *é espaço vetorial de dimensão dois sobre* $\mathrm{GF}(4)$*, com base* $(1, x)$*.*
A seguir estão as combinações lineares da base $(1, x)$*. Cada linha mostra* $\alpha(1) + \beta(x)$*, onde* α, β *são coeficientes pertencentes ao corpo subjacente do espaço vetorial (aqui* $\mathrm{GF}(4)$*).*

$$\begin{aligned} 0 + 0(x) &= 0 \\ 1 + 0(x) &= 1 \\ 0 + 1(x) &= x \\ 1 + 1(x) &= x + 1 \\ 0 + x(x) &= x^2 \\ 1 + x(x) &= x^2 + 1 \\ x + x(x) &= x^2 + x \\ x + 1 + (x)(x) &= x^2 + x + 1. \end{aligned}$$

Também é verdade[1] *que* $\mathrm{GF}(8)$ *é extensão de grau quatro de* $\mathrm{GF}(2)$*. E, de acordo com o Teorema13.2, Claramente,*

$$[\mathrm{GF}(8) : \mathrm{GF}(2)] = [\mathrm{GF}(8) : \mathrm{GF}(4)]\ [\mathrm{GF}(4) : \mathrm{GF}(2)] = (2)(2) = 4. \qquad \blacktriangleleft$$

13.2 Corpos Quadráticos

Os corpos quadráticos são extensões de $\mathbb{Q}$, de grau dois.

Definição 13.3 (corpo quadrático)**.** *Seja* $d \in \mathbb{Z}$ *livre de quadrados, com* $|d| > 1$*. Então*

$$\mathbb{Q}[\sqrt{d}] = \left\{ a + b\sqrt{d} \ : \ a, b \in \mathbb{Q} \right\}$$

Quando $d > 0$*, dizemos que* $\mathbb{Q}[\sqrt{d}]$ *é um* ***corpo quadrático real****; quando* $d < 0$ *dizemos que* $\mathbb{Q}[\sqrt{d}]$ *é um corpo* ***quadrático imaginário****.* $\blacktriangleleft$

É simples verificar que $\mathbb{Q}[\sqrt{d}]$ é de fato um corpo, e claramente, $\mathrm{Q}[\sqrt{d}]$ é espaço vetorial sobre Q, com base $(1, \sqrt{d})$.

Exemplo 13.6. *Com* $d = 2$*, há o corpo quadrático*

$$\mathbb{Q}[\sqrt{2}] = \left\{ a + b\sqrt{2} \ : \ a, b \in \mathbb{Q} \right\}.$$

Já com $d = -1$*,*

$$\mathbb{Q}[i] = \{a + bi \ : \ a, b \in \mathbb{Q}\}. \qquad \blacktriangleleft$$

[1] Verifique!

Exemplo 13.7. *Com* $d = 6$*, o corpo quadrático é*

$$\mathbb{Q}[\sqrt{6}] = \mathbb{Q}[\sqrt{2}\sqrt{3}] = \left\{ a + b\sqrt{2}\sqrt{3} \ : \ a, b \in \mathbb{Q} \right\}.$$

◀

Antes de definir os conceitos de conjugado, traço e norma, damos uma motivação. Representamos os membros de $\mathbb{Q}[\sqrt{d}]$ usando um isomorfismo[2] com matrizes 2×2,

$$a + b\sqrt{d} \quad \leftrightarrow \quad \begin{pmatrix} a & bd \\ b & a \end{pmatrix}, \tag{13.1}$$

de onde chegamos naturalmente à definição 13.4.

Definição 13.4 (conjugado, norma e traço)**.** *Se Seja* $\alpha = a + b\sqrt{d} \in \mathbb{Q}[d]$*, representado usando o isomorfismo na Equação 13.1 como* $A = \left(\begin{smallmatrix} a & bd \\ b & a \end{smallmatrix}\right)$*. Os dois autovalores da matriz são* ***conjugados****, de forma que o* ***conjugado*** *de* α *é* $\overline{\alpha} = a - b\sqrt{d}$*. A* norma *de* α *é o determinante da matriz* A*,* $N(\alpha) = \alpha\overline{\alpha} = a^2 - b^2 d$*, e o* traço *de* α *é o traço da matriz* A*,* $\mathrm{Tr}(\alpha) = \alpha + \overline{\alpha} = 2a$*.*
A matriz em 13.1 é chamada de ***representação regular*** *do número* $a + b\sqrt{d}$*.* ◀

Exemplo 13.8. *Em* $\mathbb{Q}[\sqrt{2}]$*, seja* $\alpha = 3 + 4\sqrt{2}$*.*

$$\begin{aligned} N(\alpha) &= 9 - 16(2) = -23 \\ \mathrm{Tr}(\alpha) &= 6 \\ \overline{\alpha} &= 3 - \sqrt{2}. \end{aligned}$$

Ilustra-se aqui também que a norma pode ser negativa. ◀

Tendo dois autovalores diferentes, a representação regular de $z = a + b\sqrt{d}$ é sempre uma matriz diagonalizável.

Teorema 13.3. *Se* $\alpha, \beta \in \mathbb{Q}[\sqrt{d}]$*, então* $N(\alpha\beta) = N(\alpha)N(\beta)$*, e* $\mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)$*.*

Evidentemente, $\mathrm{Tr}(\alpha) = \mathrm{Tr}(\overline{\alpha})$, e $N(\alpha) = N(\overline{\alpha})$. É também simples verificar, calculando, que todo $\alpha \in \mathbb{Q}[\sqrt{d}]$ tem norma em $\mathbb{Q}$.

Teorema 13.4. *Todo* $\alpha \in \mathbb{Q}[\sqrt{d}]$ *é raiz do polinômio característico de sua representação como matriz – portanto mônico, de grau dois e com coeficientes racionais.*

[2] Se trocarmos $\mathbb{Q}$ por $\mathbb{R}$ e tomarmos $d = -1$, resulta o corpo $\mathbb{C}$ – cujos elementos $z = x + yi$ podem ser representados por matrizes $\left(\begin{smallmatrix} x & -y \\ y & x \end{smallmatrix}\right)$, onde x é a parte real e y a parte imaginária. De fato, $i^2 = -1$, e $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)^2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

Demonstração.

$$\begin{aligned}(r-\alpha)(r-\overline{\alpha}) &= r^2-(\alpha+\overline{\alpha})r+\alpha\overline{\alpha}\\ &= r^2-\mathrm{Tr}(\alpha)r+\mathrm{N}(\alpha)\end{aligned} \tag{13.2}$$

Este é evidentemente o polinômio característico de $\left(\begin{smallmatrix} x & yd \\ y & x\end{smallmatrix}\right)$, quando $\alpha = x+y\sqrt{d}$. □

Definição 13.5 (inteiro em corpo quadrático)**.** *Dizemos que α é **inteiro** em $\mathbb{Q}[\sqrt{d}]$ (também chamado de **inteiro quadrático**) se o polinômio 13.2, que define α, tem coeficientes em $\mathbb{Z}$.* ◀

Exemplo 13.9. *Em $\mathbb{Q}[\sqrt{2}]$, $1+3\sqrt{2}$ é inteiro, porque sua representação natural é*

$$\begin{pmatrix}1 & 6\\ 3 & 1\end{pmatrix},$$

que tem polinômio característico $x^2-2x-17$, com coeficientes em $\mathbb{Z}$. ◀

Exemplo 13.10. *Em $\mathbb{Q}[\sqrt{2}]$, $\frac{1}{2}+\frac{1}{3}\sqrt{2}$ não é inteiro, porque sua representação natural é*

$$\begin{pmatrix}1/2 & 2/3\\ 1/3 & 1/2\end{pmatrix},$$

que tem polinômio característico $x^2-x+1/36$, com coeficientes em $\mathbb{Z}$. ◀

Exemplo 13.11. *Em $\mathbb{Q}[\sqrt{5}]$, $\frac{1}{2}+\frac{1}{2}\sqrt{5}$ não é inteiro, porque sua representação natural é*

$$\begin{pmatrix}1/2 & 5\\ 5 & 1/2\end{pmatrix},$$

que tem polinômio característico $x^2-x-19/4$, e nem todos os coeficientes estão em $\mathbb{Z}$. ◀

Teorema 13.5. *Se $\alpha \in \mathbb{Q}[\sqrt{d}]$ é inteiro quadrático, então $\mathrm{N}(\alpha) \in \mathbb{Z}$ e $\mathrm{Tr}(\alpha) \in \mathbb{Z}$.*

Demonstração. Segue trivialmente da definição de inteiro quadrático. O polinômio 13.2 tem coeficientes em $\mathbb{Z}$, e tanto a norma como o traço são coeficientes. □

O Lema 13.1 será usado na demonstração do Teorema 13.6, que identifica a forma dos inteiros em $\mathbb{Q}[\sqrt{d}]$.

Lema 13.1. *Se $t^2d \in \mathbb{Z}$, e d é livre de quadrados, então $t \in \mathbb{Z}$.*

Demonstração. Seja m/n a representação do racional t como fração, já reduzida, e seja p algum primo na fatoração do denominador n. Então

$$dt^2 = d\frac{m^2}{p^2w^2},$$

e como d é livre de quadrados, não há como algum fator de d cancelar p^2. Logo, se $dt^2 \in \mathbb{Z}$ e d é livre de quadrados, então $t \in \mathbb{Z}$, como determina o enunciado. □

Teorema 13.6. *Os inteiros em $\mathbb{Q}[\sqrt{d}]$ são de uma das duas formas a seguir.*

$$\begin{cases} \left\{ x + y\sqrt{d} \ : \ x, y \in \mathbb{Z} \right\} & \text{se } d \neq 4k+1 \\ \left\{ \dfrac{x + y\sqrt{d}}{2} \ : \ x, y \in \mathbb{Z}, x, y \text{ tem mesma paridade} \right\} & \text{se } d = 4k+1 \end{cases}$$

Demonstração. ($\Rightarrow$) Primeiro mostramos que os elementos das duas formas dadas são realmente inteiros quadráticos.

Suponha que $\alpha = a + b\sqrt{d}$, com $a, b \in \mathbb{Z}$, então o traço e a norma de α são $2a$ e $a^2 = b^2 d$, inteiros – portanto os coeficientes do polinômio característico associado são inteiros.

Agora suponha que $\alpha = \frac{a+b\sqrt{d}}{2}$, sendo que a e b tem a mesma paridade. O traço é $\mathrm{tr}(\alpha) = a$. A norma é

$$\begin{aligned} N(\alpha) &= \frac{a}{2} + \frac{b}{2}\sqrt{d}\frac{a}{2} - \frac{b}{2}\sqrt{d} \\ &= \frac{a^2 - b^2 d}{4} \\ &= \frac{a^2 - b^2(4k+1)}{4} \\ &= \frac{a^2 - 4kb^2 - b^2}{4} \\ &= \frac{a^2 - b^2}{4} - kb^2 \\ &= \frac{(a+b)(a-b)}{4} = kb^2 \end{aligned}$$

como a e b tem a mesma paridade, então tanto $a + b$ como $a - b$ são pares, e $4 \mid (a+b)(a-b)$. Logo, $N(\alpha) \in \mathbb{Z}$.

($\Leftarrow$) Mostramos agora que qualquer inteiro quadrático deve ser de uma das duas formas.

Seja $\alpha = a + b\sqrt{d}$ um inteiro quadrático. Queremos mostrar que os coeficientes do polinômio característico de α são inteiros, ou seja, mostrar que a norma e o traço de α são inteiros.

O traço de α é $2a$, logo a pode ser um inteiro ou metade de um inteiro.

A norma de α é $a^2 - b^2 d$.

Suponha que x seja igual a $a/2$, com $a \in \mathbb{Z}$. Então

$$\left(\frac{a}{2}\right)^2 + y^2 d \in \mathbb{Z}$$
$$\frac{a^2}{4} + y^2 d \in \mathbb{Z}$$
$$a^2 + (4y^2)d \in 4\mathbb{Z}$$
$$a^2 + (2y)^2 \in 4\mathbb{Z}$$

Agora, sabemos que $a^2 \in \mathbb{Z}$, logo $(2y)^2 \in \mathbb{Z}$ também, o que significa que y pode ser inteiro ou metade de inteiro. Mas presumimos que a é ímpar, e se $y \in \mathbb{Z}$, a última equação seria uma contradição: $a^2 + (2y)^2$, ímpar, seria múltiplo de 4. Assim, $y = b/2$ para algum $b \in \mathbb{Z}$.

$$x^2 - dy^2 = \frac{a^2}{4} - \frac{b^2}{4}d = 4k$$

Logo,

$$\begin{aligned} a^2 &\equiv db^2 \pmod 4 \\ 1 &\equiv d(1) \pmod 4, \qquad \text{(quadrados ímpares são } 1 \pmod 4\text{)} \end{aligned}$$

e temos $d \equiv 1 \pmod 4$.
Agora, suponha que $d \not\equiv 1 \pmod 4$. Da discussão anterior, vemos que x não pode ser metade de um inteiro, portanto $x \in \mathbb{Z}$. Mas como $x^2 - dy^2 \in \mathbb{Z}$, então $dy^2 \in \mathbb{Z}$, e como d é livre de quadrados, pelo Lema 13.1[3] $y \in \mathbb{Z}$. □

É interessante, após este Teorema, rever os exemplos 13.9, 13.10 e 13.11.
Por conveniência, adotaremos uma forma unificada para denotar o conjunto de inteiros em um corpo quadrático. Observamos que se $x, b \in \mathbb{Z}$ tem a mesma paridade,

$$\begin{aligned} \frac{x + b\sqrt{d}}{2} &= \frac{x - b + b + b\sqrt{d}}{2} \\ &= \frac{x-b}{2} + b\left(\frac{1+\sqrt{d}}{2}\right) \\ &= a + b\left(\frac{1+\sqrt{d}}{2}\right). \qquad (x - b \text{ é par}) \end{aligned}$$

Seja

$$\omega = \begin{cases} \sqrt{d} & \text{se } d \equiv 1 \pmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{se } d \not\equiv 1 \pmod 4 \end{cases}$$

[3] **Lema 13.1:** Se $t^2 d \in \mathbb{Z}$, e d é livre de quadrados, então $t \in \mathbb{Z}$.

Denotaremos os inteiros em um corpo quadrático $F = \mathbb{Q}[\sqrt{d}]$ por

$$\mathcal{O}_F = \mathbb{Z}[\omega] = \{a + b\omega \ : \ a, b \in \mathbb{Z}\}.$$

Teorema 13.7. *Se α e β são inteiros em $\mathbb{Q}[\sqrt{d}]$, então $\overline{\alpha}$, $\alpha+\beta$ e $\alpha\beta$ também são.*

Não é difícil perceber, a partir do Teorema 13.7, que os inteiros em um corpo quadrático F formam um anel.

Definição 13.6 (anel de inteiros quadráticos)**.** *O conjunto de inteiros quadráticos em um corpo quadrático F, com as operações usuais, é o **anel de inteiros quadráticos** de F, denotado por $\mathcal{O}_F$.* ◀

13.3 Divisibilidade

A noção de divisibilidade em $\mathbb{Z}$ se estende a inteiros quadráticos.

Definição 13.7 (divisibilidade para inteiros quadráticos)**.** *Sejam $\alpha, \beta \in \mathcal{O}_F$. Dizemos que α **divide** β (denotamos $\alpha \mid \beta$) se existe $\gamma \in \mathcal{O}_F$ tal que $\alpha\gamma = \beta$. Quando α não divide β, denotamos $\alpha \nmid \beta$.* ◀

Teorema 13.8. *Sejam $a + b\omega \in \mathbb{Z}[\omega]$ e $n \in \mathbb{Z}$. Então $n \mid \alpha$ se e somente se $n \mid a$ e $n \mid b$*

Demonstração. Se $n \mid a$ e $n \mid b$, é evidente que $n \mid \alpha = a + b\omega$. Agora presuma que $n \mid \alpha = a + b\omega$ Então

$$\begin{aligned}(a + b\omega) &= n(x + y\omega)\\ a + b\omega &= nx + ny\omega\end{aligned}$$

e $a = nx$, $b = ny$, logo $n \mid a$ e $n \mid b$. □

Relembramos a definição de unidade, desta vez aplicada a inteiros quadráticos.

Definição 13.8 (unidade)**.** *Uma **unidade** em $\mathcal{O}_F$ é um elemento com inverso em $\mathcal{O}_F$ – ou seja, γ é unidade se e somente se existe δ tal que $\gamma\delta = 1$.* ◀

Teorema 13.9. *As unidades em um corpo quadrático são os elementos com norma igual a ± 1.*

Demonstração. Usamos a definição de unidade. γ é unidade se e somente se existe δ tal que

$$\begin{aligned}\gamma\delta &= 1\\ N(\gamma\delta) &= N(1)\\ N(\gamma)N(\delta) &= 1,\end{aligned}$$

portanto a norma de qualquer unidade é ± 1.
Agora, suponha que para algum $\alpha \in \mathbb{Q}[\sqrt{d}]$, $N(\alpha) = \pm 1$.

$$\alpha\overline{\alpha} = N(\alpha)$$
$$\alpha\overline{\alpha} = \pm 1,$$

e o inverso de α é $\mp\overline{\alpha}$. □

Teorema 13.10. *As unidades em um corpo quadrático formam um grupo com a operação de multiplicação.*

Demonstração. Segue naturalmente do Teorema 13.9. □

Denotamos o grupo de unidades em $\mathcal{O}_F$ por $\mathcal{O}_F^\times$.

Teorema 13.11. *Para qualquer corpo quadrático* F, $\mathcal{O}_F \cap \mathbb{Q} = \mathbb{Z}$, *e consequentemente* $\mathcal{O}_F^\times \cap \mathbb{Q} = \{\pm 1\}$.

Demonstração. Se $\alpha \in \mathcal{O}_F \cap \mathbb{Q}$ então $\alpha = a + b\omega$, com $a, b \in \mathbb{Z}$ e $\alpha \in \mathbb{Q}$. Mas $\omega \notin \mathbb{Q}$, logo $b = 0$ e $\alpha = a \in \mathbb{Z}$.
A segunda parte do enunciado segue porque ± 1 são os únicos racionais com norma ± 1. □

Teorema 13.12. $\mathbb{Q}[\sqrt{d}]$ *tem infinitas unidades quando* $d > 0$.

Teorema 13.13. $\mathbb{Q}[\sqrt{-1}]$ *tem quatro unidades,* ± 1 *e* $\pm\sqrt{-1}$; $\mathbb{Q}[\sqrt{-3}]$ *tem seis unidades,* ± 1, $\pm(-1+\sqrt{-3})/2$ *e* $\pm(-1-\sqrt{-3})/2$; *para outros valores de* $d < 0$, $\mathbb{Q}[\sqrt{d}]$ *tem somente as duas unidades* ± 1.

Definição 13.9 (elementos irredutíveis, primos em corpo quadrático)**.** *Seja* $\alpha \in \mathcal{O}_F$. *Se toda decomposição* $\alpha = \beta\gamma$ *com* $\beta, \gamma \in \mathcal{O}$ *implica que um dos fatores,* β *ou* γ *é uma unidade, então* α *é* ***irredutível*** *em* $\mathcal{O}$.
Se, para todo elemento α *não zero e não unidade,* $\alpha \mid \beta\gamma$ *sempre implica em* $\alpha \mid \beta$ *ou* $\alpha \mid \gamma$, *então* α *é* ***primo***. ◄

Enquanto primos e irredutíveis são noções equivalentes em $\mathbb{Z}$, são diferentes em anéis de inteiros quadráticos. Por exemplo, em $\mathbb{Q}[\sqrt{3}]$ o número 13 é irredutível: não existem α, β tais que $13 = \alpha\beta$. Mas 13 não é primo, já que

$$(4+\sqrt{3})(4-\sqrt{3}) = 13,$$

e 13 divide o produto no lado esquerdo da equação – mas não divide individualmente os fatores $4 \pm \sqrt{3}$.

Teorema 13.14. *Seja* $\alpha \in \mathcal{O}_F$. *Se* $|N(\alpha)|$ *é igual a um número primo em* $\mathbb{Z}$, *então* α *é irredutível em* $\mathcal{O}_F$.

Demonstração. Segue da multiplicatividade da norma. □

Teorema 13.15. *Um elemento em um anel de inteiros quadráticos que não é zero nem unidade pode ser decomposto em produto de irredutíveis.*

A fatoração a que se refere o Teorema 13.15 pode ou não ser única, dependendo do corpo quadrático.

13.4 Corpos quadráticos e formas quadráticas

Exercícios

Ex. 322 — Prove que se α é inteiro quadrático, então $\alpha^2 + (\overline{\alpha})^2 \in \mathbb{Z}$.

Ex. 323 — Prove que $\mathbb{Q}[\sqrt{2}]$ e $\mathbb{Q}[\sqrt{3}]$ não são isomorfos.

Ex. 324 — Prove que $\mathbb{Q}[\sqrt{2}\sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$, e que consequentemente, $\mathbb{Q}[\sqrt{2}\sqrt{3}]$ é extensão de $\mathbb{Q}[\sqrt{2}]$.

Ex. 325 — Determine $\left[\mathbb{Q}[\sqrt{3}\sqrt{5}] : \mathbb{Q}[\sqrt{5}]\right]$ e $\left[\mathbb{Q}[\sqrt{3}\sqrt{5}] : \mathbb{Q}\right]$.

Ex. 326 — Prove que há infinitos irredutíveis em $\mathcal{O}_F$, para qualquer corpo infinito F.

Ex. 327 — Prove que se $\left(a + b\sqrt{d}\right)/2$ pertence um corpo contido em $\mathbb{Q}$, então $\sqrt{d}$ pertence ao mesmo corpo.

Ex. 328 — Suponha que, ao invés da representação regular que apresentamos, usemos

$$\begin{pmatrix} a & bd & 0 \\ b & a & 0 \\ 0 & 0 & a \end{pmatrix}, \quad \begin{pmatrix} a & bd & 0 \\ b & a & cd \\ 0 & c & a \end{pmatrix}.$$

Quais são as implicações? Estude traço, norma, os números representados pela matriz. Verifique como as demonstrações onde usamos traço e norma são afetadas.

Capítulo 14

Partições de um Inteiro

Este capítulo é apenas um esboço
Uma *partição* de um inteiro positivo n é uma descrição de n como soma de outros inteiros positivos: $4 = 3 + 1$ é uma partição do número 4. Uma partição é, usando aditividade, conceitualmente semelhante ao da fatoração de um número usando multiplicatividade.
Euler foi pioneiro no estudo de partições de inteiros[1].

14.1 Funções geradoras

A expansão de $(1+x)^n$ é o polinômio

$$\begin{aligned}(1+x)^n &= \binom{n}{0}x^0 + \binom{n}{1}x^1 + \cdots + \binom{n}{n-1}x^{n-1}\binom{n}{n}x^n \\ &= \sum_{j=0}^{n}\binom{n}{j}x^j\end{aligned}$$

Dizemos que $(1+x)^n$ é a *função geradora* de $\binom{n}{k}$, uma vez que $(1+n)^n$ descreve completamente os valores de $\binom{m}{k}$. Note que não demos atenção ao valor de $(1+x)^n$, mas apenas os coeficientes em sua expansão; e note também que a função geradora *determina completamente* a sequência de coeficientes. Neste Capítulo usaremos *séries formais de potencias*. Estas são semelhantes a polinômios, mas podem ter infinitos termos, e usualmente as

[1] O Capítulo 16 da primeira parte do livro Introduction in Analysin Infinitorum tem o título *De Partitione Numerorum*, onde Euler apresenta uma grande quantidade de idéias fundamentais no estudo de partições de inteiros.

Euler, Leonhard. **Introduction in Analysin Infinitorum**. [*S. l.*], 1748. O original em Latim está disponível em https://archive.org/details/bub_gb_jQ1bAAAAQAAJ/page/n21/.

tratamos como objetos algébricos – elementos que somamos e multiplicamos dentro de uma estrutura algébrica – e não como funções.

Definição 14.1 (série formal de potências)**.** *Seja* R *um anel comutativo. Então uma* ***série formal de potencias*** *na variável* x *sobre* R *é um objeto da forma*

$$\sum_{j\geq 0} a_j x^j,$$

onde $a_j \in R$.
As séries formais de potências onde os coeficientes pertencem a R *e a variável é* x *formam um anel, denotado* $R[[x]]$*.* ◀

Definição 14.2 (função geradora)**.** *Seja* $(a_n) = a_1, a_2, a_3, \ldots$ *uma sequência infinita de inteiros. Então a série formal de potências*

$$\sum_{j=0}^{\infty} a_j x^j$$

é a ***função geradora*** *da sequência* (a_n)*.* ◀

Por exemplo,

$$\frac{1}{1-x}$$

é função geradora da sequência $(1, 1, 1, \ldots)$: note que

$$\lim_{k\to\infty} \sum_{j=0}^{k} x^j = \frac{1}{1-x},$$

e os coeficientes na soma ($\sum x^j$) são todos iguais a um.
Para um segundo exemplo, a sequência $(2, 1 + 1/2, 1 + 1/3, \ldots, 1 + 1/k, \ldots)$ tem como função geradora

$$-\ln(1-x),$$

já que

$$\lim_{m\to\infty} \sum_{j=0}^{m} \left(1 + \frac{1}{j}\right) x^j = -\ln(1-x).$$

14.2 Partições

Definição 14.3 (partição de um inteiro)**.** *Uma* ***partição*** *de um inteiro positivo* n *é uma representação de* n *como soma de outros inteiros positivos. Definimos que o número zero tem somente uma partição, vazia.* ◀

Por exemplo, as partições de 4 são

$$\begin{aligned} 4 &= 1 + 1 + 1 + 1 \\ &= 2 + 1 + 1 \\ &= 2 + 2 \\ &= 3 + 1 \\ &= 4. \end{aligned}$$

Definição 14.4 ($p(n)$, quantidade de partições)**.** *Denotamos por* $p(n)$ *a quantidade total de partições do inteiro* n*. Definimos que* $p(n) = 0$ *se* $n < 0$*.* ◀

Note que a Definição 14.3 implica que $p(0) = 1$.

Definição 14.5 (representação gráfica de partições, diagrama de Ferrers)**.** *Cada partição de um inteiro pode ser representado por um* ***diagrama Ferrers****, onde cada parte é representada por uma linha, e em cada linha ficam dispostas marcas (pontos) na quantidade igual à parte.* ◀

Uma das partições de sete é $7 = 4 + 2 + 1$. O diagrama de Ferrers desta partição é

$$\begin{array}{cccc} \circ & \circ & \circ & \circ \\ \circ & \circ & & \\ \circ & & & \end{array}$$

Teorema 14.1. *Para todo* n *inteiro positivo,* $p(S_{\leq m}, n) = P(S_{\#m}, n)$.

Demonstração. Há uma bijeção entre partições e partições conjugadas: para cada partição com no máximo m partes, há exatamente uma conjugada com partes não maiores que m – basta observer a representação gráfica das partições. □

Teorema 14.2.

$$p_1(\hat{\mathbb{N}}, n) - p_2(\hat{\mathbb{N}}, n) = \begin{cases} (-1)^s & n = s\frac{(3s\pm1)}{2} \\ 0 & \text{caso contrário.} \end{cases}$$

Teorema 14.3. *Para todo* n *inteiro positivo,* $p(\hat{I}, n) = p(\hat{\mathbb{N}}_1, n)$.

É interessante estudar duas demonstrações diferentes deste Teorema.

Demonstração. Suponha que uma partição de um número n tenha apenas partes ímpares. Então

$$n = 1 + \ldots + 1 + 3 + \ldots + 3 + \ldots + (2k+1) + \ldots + (2k+1). \qquad (14.1)$$

$$n = 1(s_1) + 3(s_2) + \ldots + (2k+1)(s_{2k+1})$$

Cada um dos termos pode ser representado em base dois, *e como nesta partição só há partes ímpares, o número dois não aparece em qualquer das partes, de forma que as representações em base 2 são distintas e não tem fatores em comum.*

$$n = (1)2^{r_1} + (3)2^{r_2} + \ldots + 2k + 1(s^{r_{2k+1}}). \tag{14.2}$$

Então, para cada partição contendo partes ímpares, existe uma partição com partes distintas.

Observamos que toda partição tem parte distintas, quando posta na base 2 ficará na forma da Equação 14.2, e poderá ser transformada, revertendo os passos, em partição com partes ímpares, como na Equação 14.1 □

Teorema 14.4. *Sejam n um inteiro positivo e $S \in \mathbb{N}$. Então*

$$\sum_{n=0}^{\infty} p(\hat{S}, n)x^n = \prod_{n \in S} \frac{1}{1-x^n}.$$

Demonstração. A série geométrica $a + ax + ax^2 + ax^3 + \cdots$, quando $|x| < 1$, converge para o valor

$$\frac{a}{1-r},$$

portanto, usando $r = x^n$,

$$\begin{aligned}
\prod_{n \in S} \frac{1}{1-x^n} &= \prod_{n \in S} \left((x^n)^0 + (x^n)^1 + (x^n)^2 + (x^n)^3 + \ldots\right) \\
&= \prod_{n \in S} \left(1 + x^n + x^{2n} + x^{3n} + \ldots\right) \\
&= \sum_{(k_1, \ldots, k_j) \in \mathbb{Z}^j} x^{s_1 k_1 + \ldots + s_j k_j},
\end{aligned}$$

onde $S = \{s_1, s_2, \ldots, s_j\}$.

O número de vezes que x^n aparece no somatório é o número de soluções distintas para

$$n = s_1 k_1 + \ldots + s_j k_j, \tag{14.3}$$

sendo cada solução uma partição de n em $\hat{S}$. Tendo definido uma bijeção entre as soluções da equação 14.3 e as partições de cada n em $\hat{S}$, temos finalmente

$$\sum_{n=0}^{\infty} p(\hat{S}, n)x^n = \prod_{n \in S} \frac{1}{1-x^n}. \tag{14.4}$$

Falta, para completar a demonstração, tratar da convergência dos dois lados da igualdade.

No lado esquerdo da equação 14.4, a soma $\sum_{n=0}^{\infty} p(\hat{S}, n)x^n$ converge:

$$\begin{aligned}\sum_{n=0}^{s_p} p(\hat{S}, n)x^n &\leq \prod_{i=1}^{p} \frac{1}{1-x^{s_i}} \\ &< \prod_{i=1}^{\infty} \frac{1}{1-x^i}\end{aligned}$$

E o último produto converge.
No lado direito da equação 14.4, $\left(1 + x^n + x^{2n} + x^{3n} + \dots\right)$ é convergente quando $|x| < 1$, e $\prod_{n\in S}\left(1 + x^n + x^{2n} + x^{3n} + \dots\right)$ é, portanto, produto finito de séries convergentes.
Veja também que

$$\lim_{m\to\infty} \prod_{i=1}^{p} \frac{1}{1-x^{s_i}} = \prod_{i=1}^{\infty} \frac{1}{1-x^i}$$

e

$$\sum_{n=0}^{\infty} p(\hat{S}, n)x^n \geq \prod_{i=1}^{p} \frac{1}{1-x^{s_i}}. \qquad \square$$

14.3 Crescimento de $p(n)$

Teorema 14.5. *Para todo inteiro positivo* n*,*

$$s^{\lfloor\sqrt{n}\rfloor} < p(n) < e^{\pi\sqrt{\frac{2n}{3}}}.$$

14.4 Exercícios

Ex. 329 — Prove que a quantidade de partições auto-conjugadas de um inteiro positivo n é igual à quantidade de partições com partes ímpares distintas desse mesmo inteiro.

Ex. 330 — Mostre algum $\hat{S}$ tal que $p(\hat{S}, n)$ seja igual à quantidade de partições onde a distância entre cada duas partes é no mínimo 3, ou prove que não existe um $\hat{S}$ com esta propriedade.

Capítulo 15

Frações Contínuas

No Capítulo 2 realizamos a construção conceitual dos números naturais, inteiros e racionais. Os racionais, no entanto, não são suficientes sequer para a simples descrição de grandezas físicas fundamentais. Tome por exemplo a medida da diagonal de um quadrado de lado unitário – seu valor, $\sqrt{2}$, não é racional; outro exemplo simples está na razão entre perímetro e o diâmetro de qualquer círculo, π, que também não é racional. Faz-se necessário, portanto, definir rigorosamente um conjunto de números mais amplo que os racionais (e ao definir um novo conjunto, definimos sobre ele as operações de soma e multiplicação, obtendo assim uma nova estrutura algébrica). Trataremos de frações contínuas, números definidos como frações recursivas, e com elas obteremos umnovo modelo para os racionais, identificaremos os irracionais e construiremos um modelo para os reais.

Frações contínuas tem importância maior que a de uma simples ferramenta para mais uma construção dos reais[1]. Elas tem interessantes aplicações, e examinaremos algumas delas.

15.1 Frações Contínuas Finitas e Números Racionais

Revemos mais uma vez a seguir os passos do algoritmo de Euclides para cálculo do MDC. Desta vez, mudamos a notação: denotamos os restos por

[1] Há mais de vinte maneiras de construir $\mathbb{R}$. Um *survey*:

Weiss, Ittay. Survey Article: The Real Numbers - a survey of constructions. **Rocky Mountain Journal of Mathematics**, v. 45, n. 3, 2015. Também disponível em `https://arxiv.org/abs/1506.03467`.

x_i e os quocientes por y_i.

$$\begin{aligned} x_0 &= y_1 x_1 + x_2 && (x_0 \div x_1 = y_1, \text{ resto } x_2) \\ x_1 &= y_2 x_2 + x_3 \\ &\vdots \\ x_{n-1} &= y_n x_n \ (+0) \end{aligned}$$

No desenvolvimento do algoritmo estendido de Euclides, nosso foco de interesse eram os restos – isolamos as variáveis que representam os restos para descrever o último resto como função dos dois números iniciais. Agora nos interessam os quocientes y_i.

$$y_i = \frac{x_{i-1}}{x_i} - \frac{x_{i+1}}{x_i}$$

Definimos

$$q_i = \frac{x_i}{x_{i+1}}$$

E obtemos

$$q_i = y_i + \frac{1}{q_{i+1}}$$

Então

$$\begin{aligned} q_0 &= y_0 + \frac{1}{q_{i+1}} \\ &= y_0 + \cfrac{1}{y_1 + \cfrac{1}{q_2}} \\ &\vdots \\ &= y_0 + \cfrac{1}{y_1 + \cfrac{1}{y_2 + \quad \ddots \quad + \cfrac{1}{y_n + \cfrac{1}{y_{n+1}}}}} \end{aligned}$$

Por exemplo, se calcularmos $\mathrm{MDC}(111, 495)$,

$$\begin{aligned} 495 &= 4(111) + 51 \\ 111 &= 2(51) + 9 \\ 51 &= 5(9) + 6 \\ 9 &= 1(6) + 3 \\ 6 &= 2(3) + 0 \end{aligned}$$

teremos da primeira linha que

$$\frac{495}{111} = 4 + \frac{51}{111},$$

obtendo assim a parte inteira da fração. Se fizermos o mesmo com $51/111$, e assim sucessivamente, chegaremos a

$$\frac{495}{111} = 4 + \cfrac{1}{2 + \cfrac{1}{5 + \cfrac{1}{1 + \cfrac{1}{2}}}}$$

Esta é uma representação do racional $495/111$ na forma de fração contínua.

Definição 15.1 (fração contínua)**.** *Uma* ***fração contínua finita***[2] *é uma expressão da forma*

$$x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \quad \ddots \quad + \cfrac{1}{x_n}}}$$

também denotada[3] $[x_0; x_1, x_2, \ldots, x_n]$*. Os* x_i *são os* ***coeficientes parciais***

[2] Para uma extensa revisão da história das frações contínuas, veja o livro de Claude Brezinski.

Brezinski, Claude. **History of Continued Fractions and Padé Approximants**. Berlin Heidelberg: Springer-Verlag, 1991.

[3] Há outras notações além das duas apresentadas. Por exemplo, $x_0 + \frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} + \ldots$ (posicionando o operador de soma alinhado com os denominadores) ou, no estilo de Alfred Pringsheim, $x_0 + \frac{1}{|x_1|} + \frac{1}{|x_2|} + \frac{1}{|\ldots|} + \frac{1}{|x_n|}$, e também usando o operador $\mathcal{K}$, introduzido por Gauss,

$$x_0 + \operatorname*{\mathcal{K}}_{m=1}^{\infty} \left(\frac{1}{x_m}\right) = \frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} + \cdots,$$

mas não comum hoje. Como curiosidade, a notação para frações contínuas usada por Pietro Cataldi em 1613 é: $x_0 \cdot \,\&\, \frac{x_1}{y_1.} \,\&\, \frac{x_2}{y_2.} \,\&\, \frac{x_2}{y_2.} \cdots$.

da fração contínua[4].
Se x_i *é inteiro quando* $i > 0$*, dizemos que a fração contínua é* ***simples***. ◀

Frações contínuas finitas representam números racionais: expandimos $495/111$, por exemplo, até chegar a uma fração contínua. Fazemos agora o oposto: a partir de $[4;1,5,4]$ obtemos um racional.

$$[4;1,5,4] = 4 + \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{1}{4}}} = \frac{121}{25}.$$

Teorema 15.1. *Toda fração contínua finita representa um número racional.*

Demonstração. Segue claramente da maneira como frações contínuas finitas são definidas – apenas soma e divisão são usadas, e estas operações são fechadas em $\mathbb{Q}$. □

Teorema 15.2. *Todo racional pode ser representado por frações contínuas finitas*

Demonstração. Executamos o algoritmo de Euclides com o racional a/b, e obteremos sua expansão em fração contínua. Como o algoritmo de Euclides sempre para, a expansão em fração contínua sempre será finita. □

Mesmo racionais que tem representação infinita em base dez (como $1/3 = 0.3333\ldots$, por exemplo) tem representação finita como fração contínua.
Nos falta investigar a unicidade da representação de racionais como frações contínuas. Interessantemente, a representação de racionais como frações contínuas não é única: há *exatamente* duas expansões para cada racional,

Cataldi, Pietro Antonio. **Trattato del modo brevissimo di trouare la radice quadra delli numeri, et regole da approssimarsi di coninuo al vero nelle radice delli numeri non quadrati, con le cause, et inventioni loro. Et anco il modo di pigliarne la radice cuba, applicando il tutto alle operationi militari et altre**. [*S. l.: s. n.*], 1613. Sim, o título tem 48 palavras. Disponível em `https://archive.org/details/hin-wel-all-00000163-001/page/n8/mode/2up`.

[4] Falamos dos x_i porque o numerador é sempre um, mas também se pode considerar frações contínuas com numeradores diferentes de um, da forma $x_0 + \mathcal{K}_{m=1}^{\infty}\left(\frac{x_m}{y_m}\right) = \frac{x_1}{y_1} + \frac{x_2}{y_2} + \frac{x_3}{y_3} + \ldots$, ou seja,

$$x_0 + \cfrac{x_1}{y_1 + \cfrac{x_2}{y_2 + \cfrac{x_3}{y_3 + \ddots}}}.$$

Faremos isto quando tratarmos da irracionalidade de π (na Seção 15.7).

mas isto já nos serve. Por exemplo,

$$[1;1,5] = 1 + \frac{1}{1+\frac{1}{5}}, \qquad [1;1,4,1] = 1 + \frac{1}{1+\frac{1}{4+\frac{1}{1}}},$$

e ambas são evidentemente iguais (as duas valem $11/6$).

O Lema 15.1 mostra que é trivial determinar o inverso de uma fração contínua; ele será útil logo mais na demonstração da unicidade da representação.

Lema 15.1. *Se* $p > q$*, e* $p/q = [x_0; x_1, x_2, \ldots, x_n]$*, então o inverso* q/p *é* $[0; x_0, x_1, x_2, \ldots, x_n]$.

Demonstração.

$$\begin{aligned}
\frac{q}{p} &= \frac{1}{p/q} \\
&= \frac{1}{[x_0; x_1, x_2, \ldots, x_n]} \\
&= \cfrac{1}{x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \quad \ddots \quad + \cfrac{1}{x_n}}}} \\
&= [0; x_0, x_1, x_2, \ldots, x_n]
\end{aligned}$$

□

Já podemos afirmar que um racional só pode ser representado por uma única fração contínua (com último quociente diferente de um).

Lema 15.2. *Se duas frações contínuas simples* $[x_0; x_1, x_2, \ldots, x_r]$ *e* $[y_0; y_1, y_2, \ldots, y_s]$ *representam o mesmo número racional com* $x_r \neq 1$ *e* $y_s \neq 1$*, então* $r = s$ *e* $x_i = y_i$ *para todo* $0 \leq i \leq r$.

É importante que tenhamos definido que $x_r \neq 1$ e $y_s \neq 1$, porque já sabemos que com o último quociente parcial igual a um teríamos uma representação extra de cada número.

Demonstração. Suponha que $a = [x_0; x_1, x_2, \ldots, x_r] = [y_0; y_1, y_2, \ldots, y_s]$. Observe que

$$a = x_0 + [0; x_1, x_2, \ldots, x_r]$$

e também que

$$[0; x_1, x_2, \ldots, x_r] = \cfrac{1}{x_1 + \cfrac{1}{x_2 + \quad \ddots \quad + \cfrac{1}{x_r}}}$$

Como $x_i \geq 1$, o denominador é positivo e $0 < [0; x_1, x_2, \ldots, x_r] < 1$. Assim, $x_0 = \lfloor a \rfloor$. Como o mesmo vale para y_0, vemos que

$$\lfloor a \rfloor = x_0 = y_0,$$

e só precisamos mostrar que $[0; x_1, x_2, \ldots, x_r] = [0; y_1, y_2, \ldots, y_s]$.
Agora, pelo Lema 15.1

$$[0; x_1, x_2, \ldots, x_r]^{-1} = [x_1; x_2, \ldots, x_r],$$
$$[0; y_1, y_2, \ldots, y_s]^{-1} = [y_1; y_2, \ldots, y_s],$$

e pelo mesmo argumento de antes, $x_1 = y_1$. Podemos verificar portanto que, por indução, teremos $x_i = y_i$ para todo i.
Quanto a r e s, claramente, se todo x_i for igual a todo y_i, suponha que $r > s$. Teríamos

$$[x_0; x_1, \ldots x_r, x_{r+1}] = [y_0; y_1, \ldots y_r, x_{r+1}] < a. \qquad \square$$

Terminamos as demonstrações dos Lemas, e finalmente enunciamos o Teorema da unicidade das representações.

Teorema 15.3. *Há exatamente duas representações de cada racional como fração contínua finita simples; e uma representação de cada racional como fração contínua finita simples com último coeficiente diferente de um.*

Demonstração. Uma fração contínua não pode representar mais que um racional, portanto basta mostrar que um racional não pode ser representado por mais que duas frações contínuas, que é o que o Lema 15.2 afirma. $\square$

15.2 Frações Contínuas Infinitas e Números Irracionais

No início do Capítulo dissemos que os racionais tem uma limitação que os torna insuficientes para medidas simples: há números que queremos representar, mas que não é possível expressar como razão entre dois inteiros.
Um exemplo de extrema simplicidade é $\sqrt{2}$, solução de $x^2 = 2$ e medida da diagonal do quadrado unitário. Sua expansão em fração contínua pode ser

obtida facilmente:

$$\begin{aligned}
\sqrt{2} &= 1 + (\sqrt{2} - 1) \\
&= 1 + \frac{1}{1+\sqrt{2}} \\
&= 1 + \frac{1}{1 + \left(1 + \frac{1}{1+\sqrt{2}}\right)} \\
&= 1 + \frac{1}{2 + \frac{1}{2+\sqrt{2}}} \\
&= 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}}}
\end{aligned}$$

Notamos que a expansão é infinita: $\sqrt{2} = [1; 2, 2, 2, \ldots]$. É interessante que como mostramos que uma fração contínua infinita representa $\sqrt{2}$, e já havíamos demonstrado que racionais sempre tem representação finita como frações contínuas, o que temos é uma prova de que $\sqrt{2}$ é irracional. Precisamos portanto definir frações contínuas infinitas, e verificar o que elas representam e o que podemos concluir a respeito desses números.

Definição 15.2 (fração contínua infinita)**.** *Uma fração contínua é **infinita** se tem infinitos quocientes parciais.* ◀

Por exemplo,

$$\begin{aligned}
e &= [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots] \\
\pi &= [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, \ldots] \\
\phi &= [1; 1, 1, 1, 1, 1, 1, 1, 1, 1, \ldots] \\
\tan(1) &= [1; 1, 1, 3, 1, 5, 1, 7, 1, 9, 1, 11, \ldots] \\
\tanh(1) &= [0; 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, \ldots] \\
\sqrt{2} &= [1; 2, 2, 2, 2, 2, 2, 2, 2, \ldots] \\
\sqrt{3} &= [1; 1, 2, 1, 2, 1, 2, 1, 2, \ldots]
\end{aligned}$$

A representação de alguns números como frações contínuas infinitas são aparentemente aleatóreas, como a de π; outras claramente apresentam padrões, como as de e, ϕ, $\sqrt{2}$ e $\sqrt{3}$. Um caso particular de número irracional que apresenta um claríssimo padrão em representação decimal é a *constante de Champernowne*, que é construída concatenando os números natu-

rais,

$$C = 0,1234567891011121314\cdots,$$

cuja representação em frações contínuas é

$$C = [0;8,9,1,149083,1,1,1,4,1,1,1,3,4,1,1,1,15,\omega,6,1,1\ldots],$$

sem padrão aparente na sequência de coeficientes (o número ω tem 166 dígitos em representação decimal[5]).

15.2.1 Convergentes

Neste texto iniciamos com um semianel ($\mathbb{N}$) e aos poucos o aumentamos para obter estruturas mais úteis: o anel $\mathbb{Z}$ e o corpo $\mathbb{Q}$ (nesse caminho passamos brevemente pelo anel sem ordem dos inteiros Gaussianos).

Há diversos números que queremos representar, mas que não estão no corpo ordenado $\mathbb{Q}$: a diagonal do quadrado de lado um; a razão entre comprimento e diâmetro de uma circunferencia, e diversos outros. Estes são números que identificamos inicialmente por *aproximações sucessivas* – sequências de racionais que aos poucos se aproximam de algum número, que no entanto não é racional (não pode ser expresso como razão de dois inteiros). Inicialmente estudamos o que acontece quando truncamos frações contínuas: tratamos dos seus *convergentes*.

Definição 15.3 (convergente)**.** *Seja* $\alpha = [a_0;a_1,a_2,\ldots]$ *um número irracional. Uma fração contínua* $[a_0;a_1,a_2,\ldots,a_k]$ *é chamada de* ***convergente*** *de* α*. Denotamos o* i*-ésimo convergente da fração contínua* $[a_0;a_1,\ldots]$ *por* p_i/q_i*, ou ainda, por* $\alpha^{(i)}$*.* ◀

[5] $\omega = 4\,575\,401\,113\,910\,310\,764\,836\,466\,282\,429\,561\,185\,996\,039\,397\,104\,575\,550\,006\,620\,043\,930\,902\,626\,592\,563\,149\,379\,532\,077\,471\,286\,563\,138\,641\,209\,375\,503\,552\,094\,607\,183\,089\,984\,575\,801\,469\,863\,148\,833\,592\,141\,783\,010\,987$.

Por exemplo, os primeiros convergentes de $\sqrt{2}$ são

$$\begin{aligned}
p_0/q_0 &= [1] = 1 \\
p_1/q_1 &= [1;2] = 1 + \frac{1}{2} = \frac{3}{2} = 1.5 \\
p_2/q_2 &= [1;2,2] = 1 + \frac{1}{2 + \frac{1}{2}} = \frac{7}{5} = 1.4 \\
p_3/q_3 &= [1;2,2,2] = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}} = \frac{17}{12} = 1.416666\ldots \\
p_4/q_4 &= [1;2,2,2,2] = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}}} = \frac{41}{29} = 1.413793\ldots
\end{aligned}$$

A sequencia não é crescente nem decrescente.

Teorema 15.4. *Se* $a = [a_0; a_1, a_2, \ldots]$ *então os convergentes* p_i/q_i *de* a *são*

$$\begin{aligned}
p_i &= a_i p_{i-1} + p_{i-2} \\
q_i &= a_i q_{i-1} + q_{i-2}
\end{aligned}$$

com

$$\begin{aligned}
p_0 &= a_0 & \qquad q_0 &= 1 \\
p_{-1} &= 1 & \qquad q_{-1} &= 0.
\end{aligned}$$

Ou ainda, em notação matricial,

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_i & p_{i-1} \\ q_i & q_{i-1} \end{pmatrix}$$

A demonstração pode ser feita por indução no índice do convergente (i).

Corolário 15.1.

$$p_i q_{i-1} - p_{i-1} q_i = (-1)^{i+1}$$

Demonstração. Segue trivialmente, já que

$$\det \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix} = -1. \qquad \square$$

Corolário 15.2. *Para qualquer* $i \geq 0$, $\operatorname{mdc}(p_i, q_i) = 1$.

Demonstração. $p_i q_{i-1} - p_{i-1} q_i = (-1)^{i+1}$, logo qualquer divisor comum de p_i e q_i é divisor de ± 1. □

Teorema 15.5. *Seja* $1 < a \in \mathbb{R}$. *Então*

$$[x_0; \ldots, x_{k-1}, a] = \frac{a p_{k-1} + p_{k-2}}{a q_{k-1} + q_{k-2}}$$

Demonstração. Por indução em k. Para a base, seja $k = 1$. Então, usando os valores de p_0, q_0, p_1, q_1 no Teorema 15.4,

$$\begin{aligned} \frac{a p_{k-1} + p_{k-2}}{a q_{k-1} + q_{k-2}} &= \frac{a x_0 + 1}{a(1) + 0} \\ &= x_0 + \frac{1}{a} \\ &= [x_0; a]. \end{aligned}$$

Para o passo, presuma que

$$[x_0; \ldots, x_{k-1}, a] = \frac{a p_{k-1} + p_{k-2}}{a q_{k-1} + q_{k-2}}$$

Então,

$$\begin{aligned} [x_0; \ldots, x_k, a] &= [x_0; \ldots, x_{k-1}, x_k + 1/a] \\ &= \frac{(x_k + 1/a) p_{k-1} + p_{k-2}}{(x_k + 1/a) q_{k-1} + q_{k-2}} \\ &= \frac{a p_k + q_{k-1}}{a q_k + q_{k-1}}. \end{aligned}$$

□

Teorema 15.6. *Para qualquer fração contínua simples,*

$$\frac{p_{i+1}}{q_{i+1}} - \frac{p_i}{q_i} = \frac{(-1)^{i+1}}{q_i q_{i+1}}$$

Demonstração. O Corolário 15.1 determina que

$$p_i q_{i-1} - p_{i-1} q_i = (-1)^{i+1}.$$

Dividindo a equação por $q_i q_{i-1}$, chegamos ao enunciado. □

Teorema 15.7. *Para qualquer fração contínua infinita simples com convergentes* p_i/q_i,

$$\left| \frac{p_i}{q_i} - \frac{p_{i-1}}{q_{i-1}} \right| \leq \frac{1}{2^i},$$

e a sequência é convergente.

Demonstração. Denote por F_i o i-ésimo número de Fibonacci. Como $q_i \geq F_i$, então $q_i q_{i+1} \geq F_i F_{i+1} \geq 2^i$, e

$$\frac{p_i}{q_i} - \frac{p_{i-1}}{q_{i-1}} \leq \frac{(-1)^i}{2^i},$$

donde se conclui que a sequência $(a)_i$ converge, já que 2^{-i} chega arbitrariamente próximo de zero. □

Teorema 15.8. *A sequência de convergentes de índice par é estritamente crescente; a sequencia de convergentes com índice ímpar é estritamente decrescente:*

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \cdots$$
$$\frac{p_1}{q_1} > \frac{p_3}{q_3} > \frac{p_5}{q_5} > \cdots$$

Definição 15.4 (valor de fração contínua simples infinita)**.** *Dizemos que o* ***valor*** *de uma fração contínua simples infinita com convergentes* p_i/q_i *é*

$$\lim_{i\to\infty} \frac{p_i}{q_i},$$

que pelo Teorema 15.7 sempre existe. ◀

Teorema 15.9. *Seja* $x = [x_0; x_1, \ldots]$ *uma fração contínua simples infinita (*x *é o valor da fração contínua, como na definição 15.4). Seja* r_k *definido indutivamente, de forma que*

$$r_0 = \lfloor x \rfloor$$
$$x = r_0 + \frac{1}{r_1}$$
$$r_i = \lfloor r_i \rfloor + \frac{1}{r_{i+1}}$$

Então

$$x = [x_0; x_1, \ldots, x_{k-1}, r_k]$$

Demonstração. Segue de maneira simples por indução em k. □

Teorema 15.10. *Para qualquer fração contínua infinita simples com convergentes* p_i/q_i *e valor* x*,*

$$\left| x - \frac{p_i}{q_i} \right| < \frac{1}{2q_i^2}.$$

Teorema 15.11. *Seja* x *um número irracional, de forma que*

$$x = [\xi_0; \xi_1; \ldots, \xi_{k-1}, x_k]$$

Então

$$x = \frac{x_k p_i + p_{i-1}}{x_k q_i + q_{i-1}}.$$

Demonstração. Segue facilmente por indução. □

Tendo demonstrado que toda fração contínua infinita converge, nos falta verificar que, partindo de um irracional, chegaremos na mesma fração contínua. Isto é garantido pelo Teorema 15.12.

Teorema 15.12. *Seja x um número irracional, cuja expansão em fração contínua tem convergentes p_i/q_i. Então*

$$x = \lim_{i\to\infty} \frac{p_i}{q_i}$$

Demonstração. Segue dos Teoremas 15.9 e 15.8, e da Definição 15.4. □

Teorema 15.13. *Duas frações contínuas infinitas simples diferentes não podem convergir para o mesmo valor.*

Se $x = [x_0; x_1, \ldots] = [y_0; y_1, \ldots]$, então $x_0 = y_0 = \lfloor x \rfloor$. Indutivamente, o mesmo vale para todos os outros coeficientes ($x_i = y_i$), e as duas frações parciais são idênticas.

15.3 Melhor aproximação

O estudo de convergentes nos permite determinar algo mais sobre frações contínuas: os convergentes são, em certo sentido, a melhor maneira possível de aproximar um número irracional. Aqui, definimos "melhor" como "tendo o menor denominador possível". A ideia é tentar obter a fração contínua mais curta possível que aproxime o número por no máximo uma dada distância.

Definição 15.5 (melhor aproximação)**.** *Dizemos que a/b é a **melhor aproximação** de um número x se*

$$|qx - p| < |bx - a|$$

implica que $q > b$. ◀

Lema 15.3. *Se a/b é melhor aproximação para um número x, então*

$$\left|x - \frac{p}{q}\right| < \left|x - \frac{a}{b}\right|$$

implica que $q > b$.

Embora possa parecer que as duas afirmações são equivalentes, não é o caso, e a recíproca não vale (um contraexemplo é pedido no Exercício 342)

Demonstração. Suponha que o enunciado não valha. Então

$$\left|x - \frac{p}{q}\right| < \left|x - \frac{a}{b}\right|$$
$$q < b$$

Multiplicando a primeira desiguladade pela segunda (ou seja, multiplicando o lado esquerdo da primeira desigualdade por q e o lad odireito por b),

$$|qx - p| < |bx - a|.$$

E a/b não seria melhor aproximação, porque p/q seria melhor. □

Teorema 15.14. *Os convergentes p_i/q_i da fração contínua de qualquer $x \in \mathbb{R}$ são uma sequência de melhores aproximações para x.*

Demonstração. Como $q_{i+1} > q_i$, concluímos que $q_{i+1} \geq 2$. Sabemos que

$$\left|x - \frac{p_i}{q_i}\right| < \frac{1}{2q_i^2}.$$

Agora suponha que p/q seja melhor aproximação. com $q < q_i$.

$$\begin{aligned}
\left|\frac{p}{q} - \frac{p_i}{q_i}\right| &\leq \left|\frac{p}{q} - x\right| + \left|x - \frac{p_i}{q_i}\right| && \text{(desigualdade de triângulo)} \\
&\leq 2\left|x - \frac{p_i}{q_i}\right| && (p/q \text{ mais próximo de } x \text{ – Lema 15.3}) \\
&< \frac{1}{q_i^2}.
\end{aligned}$$

No entanto,

$$\left|\frac{p}{q} - \frac{p_i}{q_i}\right| = \left|\frac{pq_i - p_i q}{q_i q}\right| > \frac{1}{q_i q} \geq \frac{1}{q_i^2}.$$

Como chegamos a uma contradição, a suposição de que p/q existe é falsa. □

Teorema 15.15. *Se a/b é uma melhor proximação para um número x, então a/b é convergente na expansão de x em fração contínua.*

Demonstração. Suponha que a/b seja melhor aproximação para x. Analisamos três casos, (i) $a/b < x_0$; (ii) a/b fica entre dois convergentes, x_{i-1}, x_{i+1}, e (iii) $a/b > p_1/q_1$.

(i) É impossível que $a/b < a_0$, porque se assim fosse, 1 seria melhor aproximação do que a/b:

$$|(1)x - x_0| < \left|x - \frac{a}{b}\right| \leq |bx - x|. \qquad (1 \leq b)$$

(ii) Se a/b está entre dois convergentes, então

$$\left|\frac{a}{b} - \frac{p_{k-1}}{q_{k-1}}\right| = \left|\frac{aq_{k-1} - bp_{k-1}}{bq_{k-1}}\right| \geq \frac{1}{bq_{k-1}}$$
$$\left|\frac{a}{b} - \frac{p_{k-1}}{q_{k-1}}\right| < \left|\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}}\right| = \frac{1}{q_k q_{k-1}}$$

o que determina, claramente, que

$$q_k < b.$$

Mostramos que $q_k < b$ porque queremos mostrar que p_k/q_k seria melhor aproximação do que a/b.

Continuamos, observando que

$$\left|x - \frac{a}{b}\right| \geq \left|\frac{p_{k+1}}{q_{k+1}} - \frac{a}{b}\right|$$
$$\geq \frac{1}{bq_{k+1}}$$

Multiplicando a desigualdade por b,

$$|bx - a| \geq \frac{1}{q_{k+1}},$$

Mas já temos estabelecido que

$$\left|x - \frac{p_k}{q_k}\right| < \frac{1}{q_k q_{k+1}}$$
$$|q_k x - p_k| \leq \frac{1}{q_{k+1}},$$

então

$$|q_k x - p_k| \leq |bx - a|,$$

e a/b não pode ser melhor aproximação, porque $p_k q_k$ é melhor.

(iii) Se $a/b > p_1/q_1$, então a distância de x até a/b é maior do que até p_1/q_1:

$$\left|x - \frac{a}{b}\right| > \left|\frac{p_1}{q_1} - \frac{a}{b}\right| \geq \frac{1}{bq_1}$$

Então, multiplicando por b,

$$|bx - a| > \frac{1}{q_1} = \frac{1}{x_1}$$

Pode-se verificar faclimente que

$$|(1)x - x_0| \leq \frac{1}{x_1},$$

Mas neste caso 1 seria melhor aproximação do que a/b:

$$|bx - a| > |(1)x - x_0| \qquad (1 \leq b)$$

Nos três casos chegamos a contradições, portanto a/b precisa ser um dos convergentes na expansão de x. □

Teorema 15.16 (de Hurwitz)**.** *Na expansão em fração contínua de qualquer número irracional x, pelo menos um a cada três convergentes p/q são tais que*

$$\left| x - \frac{p}{q} \right| < \frac{1}{q^2\sqrt{5}}.$$

15.4 Frações Contínuas Periódicas

Há frações contínuas que apresentam padrões recorrentes. Por exemplo, em $[1; 1, 2, 1, 2, \dots]$ o padrão "$1, 2$" se repete indefinidamente. Os números com expansão em frações contínuas contendo estes padrões são exatamente as soluções irracionais para equações quadráticas.

Definição 15.6. *Uma fração contínua é **eventualmente periódica** se, para todo i maior que algum n, o quociente parcial x_i é igual a x_{i_t}, onde t é o período.*
Denotamos por $[x_0; x_1; x_2, \dots, \overline{x_n, \dots, x_{n+t}}]$ a fração contínua eventualmente periódica, onde o período é $x_n, \dots, x_{n_t}$. ◀

Assim, $[1; \overline{1, 2}]$ denota a fração contínua que mencionamos no primeiro parágrafo desta seção, em que o padrão "$1, 2$" é repetido infinitas vezes.

Definição 15.7 (irracional quadrático)**.** *Um **irracional quadrático** é uma solução irracional para uma equação quadrática.* ◀

Um exemplo de irracional quadrático é $\sqrt{2}$, cuja expansão, $[1; \overline{2}]$, já derivamos na Seção 15.2.
Como outro exemplo, a solução de $x^2 - x - 1 = 0$ é a razão áurea, ϕ, com expansão em fração contínua igual a $[1; \overline{1}]$

Teorema 15.17. *Toda fração contínua eventualmente periódica representa um irracional quadrático.*

Demonstração. Seja

$$x = [\xi_0; \xi_1, \ldots, \overline{\xi_k \ldots, \xi_n}]$$

Escrevemos somente a parte periódica, e chegamos a

$$x_k = [\xi_k; \ldots, \xi_n, x_k]$$
$$x_k = \frac{x_k p_n + p_{n-1}}{x_k q_n + q_{n-1}}$$

Esta última equação é claramente quadrática em x_k. Temos agora $x = [x_0; x_1; \ldots, x_k]$, onde x_k é da forma $(\alpha + \sqrt{\beta})/\gamma$, e pode-se facilmente verificar que x também deve necessariamente ser dessa forma. □

Teorema 15.18. *A expansão em fração contínua de qualquer irracional quadrático é eventualmente periódica.*

Demonstração. Seja $[\xi_0; \xi_1, \ldots]$ a expansão de x em fração contínua, e $x_k = [\xi_k; \xi_{k+1}, \ldots]$. Suponha que x é raiz de uma equação quadrática, ax^2+bx+c. Então, pelo Teorema 15.11[6],

$$x = \frac{x_k p_{k-1} + p_{k-1}}{x_k q_{k-1} - q_{k-2}},$$

e

$$a\left(\frac{x_k p_{k-1} + p_{k-1}}{x_k q_{k-1} - q_{k-2}}\right)^2 + b\left(\frac{x_k p_{k-1} + p_{k-1}}{x_k q_{k-1} - q_{k-2}}\right) + c = 0$$
$$a(x_k p_{k-1} + p_{k-1})^2 + b(x_k p_{k-1} + p_{k-1})(x q_{k-1} - q_{k-2}) + c(x q_{k-1} - q_{k-2}) = 0$$

Uma mudança de variável transforma esta equação em

$$A_k x_k^2 + B_k x_k + C_k = 0,$$

[6] **Teorema 15.11:** Seja x um número irracional, de forma que

$$x = [\xi_0; \xi_1; \ldots, \xi_{k-1}, x_k]$$

Então

$$x = \frac{x_k p_i + p_{i-1}}{x_k q_i + q_{i-1}}.$$ □

com

$$\begin{aligned} A_k &= ap_{k-1}^2 + bp_{k-1}q_{k-1} + cq_{k-1}^2 \\ B_k &= 2ap_{k-1}p_{k-2} + b(p_{k-1}q_{k-2} + p_{k-2}q_{k-1}) + 2cq_k + q_{k-2} \\ C_k &= ap_{k-3}^2 + bp_{k-3}q_{k-3} + cq_{k-2}^2 \\ &= A_{k-1} \end{aligned}$$

Definimos, portanto, sequências de coeficientes A_k, B_k, C_k, que descrevem os convergentes de x.

O discriminante $\Delta_k = B_k^2 - 4A_kC_k$ é igual ao discriminante da forma original, $\Delta = b^2 - 4ac$, e não depende de k.

$$\left| x - \frac{p_i}{q_i} \right| < \frac{1}{2q_i^2}.$$

logo

$$p_{k-1} = xq_{k-1} + \frac{|z_{n-1}|}{q_{n-1}} \qquad (|z-1| < 1)$$

Assim, A_k pode ser reescrito como

$$\begin{aligned} A_k &= a\left(xq_{k-1} + \frac{z_{k-1}}{q_{k-1}}\right)^2 + b\left(xq_{k-1} + \frac{z_{k-1}}{q_{k-1}}\right)q_{k-1} + cq_{k-1}^2 \\ &= \left(ax^2 + bx + c\right)q_{k-1}^2 + 2axz_{k-1} + a\frac{z_{k-1}}{q_{k-1}^1} + bz_{k-1} \\ &= 2axz_{k-1} + a\frac{z_{k-1}^2}{q_{k-1}^1} + bz_{k-1} \qquad (ax^2 + bx + c = 0) \end{aligned}$$

Então, como $|z_{k1}| < 1$,

$$|A_k| = \left| 2axz_{k-1} + a\frac{z_{k-1}^2}{q_{k-1}^2} + bz_{k-1} \right| < 2|ax| + |a| + |b|,$$

ou seja, $|A_k|$ é limitado por uma expressão que depende apenas de a, x e b, e portanto é consatnte (não depende de k). Como $C_k = A_{k-1}$, C_k também é limitado.

Como $\Delta_k = \Delta$ é constante e tanto A_k como B_k são limitados, então $B_k = \sqrt{\Delta - 4A_kC_k}$ também é limitado superiormente. Mais ainda – como A_k, B_k e C_k são inteiros, e as sequências são infinitas, pelo princípio da casa dos pombos, em algum momento haverá $A_k = A_{k+t}$, $B_k = B_{k+t}$ e $C_k = C_{k+t}$. E como o próximo elemento de cada sequência (A_k, B_k, C_k) depende somente dos anteriores, ela será eventualmente periódica.

15.5 Construção de $\mathbb{R}$ com frações contínuas

Gostaríamos de incluir os números irracionais (que surgem em diversos problemas e mensurações físicas) no corpo que estamos usando, e isto é equivalente a incluir "o elemento para o qual convergem" estas aproximações a que demos o nome de convergentes.

Definição 15.8 (métrica; espaço métrico)**.** *Uma* ***métrica*** *sobre um conjunto* A *é uma função* $d : A \times A \to \mathbb{R}$*, tal que para todos* $x, y, z \in A$*,*

(i) $x(x, y) \geq 0$

(ii) $d(x, y) = 0$ *se e somente se* $x = y$

(iii) $d(x, y) = d(y, x)$

(iv) $d(x, z) \leq d(x, y) + d(y, z)$

Um conjunto onde se define uma métrica é chamado de ***espaço métrico****.* ◀

Definição 15.9 (sequência de Cauchy)**.** *Uma* ***sequência*** *é* ***de Cauchy*** *em um espaço métrico se, para* N *suficientemente grande, todos os termos posteriores a* N *são arbitrariamente próximos entre si, usando a métrica daquele espaço.* ◀

Exemplo 15.1. *Em* $\mathbb{Q}$*, usando a métrica* $d(a, b) = |a - b|$*, a sequência* $a_n = 2^{-n}$ *é uma sequência de Cauchy. Dado qualquer* $\varepsilon > 0$*, existe* N *tal que para quaisquer* $n, k > N$*,*

$$|a_n - a_k| < \varepsilon,$$

bastando tomar $N = -(\log_2(\varepsilon)) + 1$*, de forma que* $2^{-N+1} < \varepsilon$*. Se* $n, k > N$*, então*

$$\begin{aligned} |a_n - a_k| &= \left| \frac{1}{2^n} - \frac{1}{2^{-k}} \right| \\ &< \frac{1}{2^n} + \frac{1}{2^k} \\ &< \frac{1}{2^N} + \frac{1}{2^N} \\ &< \frac{1}{2^{N-1}} \\ &< \varepsilon. \end{aligned}$$

◀

Exemplo 15.2. *Em* $\mathbb{Q}$*, com a distância usual, as sequências* $a_n = (-1)^n$ *e* $b_n = \sum_{j=1}^{n} 1/j$ *não são de Cauchy, porque não convergem.* ◀

Definição 15.10 (espaço métrico completo)**.** *Um espaço métrico* A *é* ***completo*** *se toda sequência de Cauchy em* A *converge para algum elemento também em* A*.* ◀

Os racionais com a métrica $d(x,y) = |x-y|$ são um espaço métrico que não é completo: a sequência de Cauchy

$$\begin{aligned}&[1]\\&[1;2]\\&[1;2;2]\\&[1;2;2,2]\\&\quad\vdots\end{aligned}$$

não converge para um racional, porque sabemos que $[1;\overline{2}] = \sqrt{2} \notin \mathbb{Q}$.

A seguir mostramos que, partindo das frações contínuas finitas (que representam os racionais), podemos construir um modelo para os reais, incluindo no conjunto as frações contínuas infinitas. Com isso toda sequências de Cauchy convergirá para um elemento no conjunto. Obteremos um corpo ordenado que também é espaço métrico completo – e que chamaremos de *corpo ordenado compelto*.

Definimos um símbolo ω tal que $\omega > n$ para todo $n \in \mathbb{N}$, e assim podemos denotar todas as frações contínuas como infinitas,

$$[a_0; a_1, a_2, \ldots, a_n] \;\to\; [a_0; a_1, a_2, \ldots, a_n, \omega, \omega, \ldots],$$

desde que os coeficientes ω estejam sempre à direita de todos os outros.

Sejam $a \neq b$,

$$\begin{aligned}a &= [a_0; a_1, a_2, \ldots],\\ b &= [b_0; b_1, b_2, \ldots],\end{aligned}$$

e $k = k(a,b)$. Claramente,

$$a < b \text{ se e somente se } \begin{cases} a_k < b_k & \text{se } 2 \mid k \\ a_k > b_k & \text{se } 2 \nmid k \end{cases}$$

Claramente, se $a < b$. então

$$\begin{aligned}a^{(2i)} &< b^{(2i)}\\ a^{(2i+1)} &< b^{(2i+1)}\end{aligned}$$

O Teorema a seguir é de G. J. Rieger, que propôs a construção dos reais com frações contínuas:

Teorema 15.19. *Seja* K *o conjunto de todas as frações contínuas (finitas e infinitas). Se* $\emptyset \neq M \subset K$ *e* M *é limitado superiormente, então* M *tem*

supremo. Mais ainda – para toda fração contínua a*,*

$$a = \sup\left\{a^{(2i)} \ : \ i \geq 0\right\}.$$

O Teorema 15.19 garante que toda sequência de Cauchy no conjunto das frações contínuas converge para uma fração contínua – temos portanto um espaço métrico completo.
A operação de soma e o inverso aditivo são definidos a seguir.

$$\begin{aligned} a + b &= \sup\left\{a^{(2n)} + b^{(2n)} \ : \ n \geq 0\right\} \\ -a &= \sup\left\{-a^{(2n+1)} \ : \ n \geq 0\right\} \end{aligned}$$

Valor absoluto e multiplicação:

$$\begin{aligned} |a| &= \sup\{a, -a\} \\ ab &= \begin{cases} \sup\left\{a^{(2n)}b^{(2n)} \ : \ n \geq 0\right\} & a \geq 0, b \geq 0 \\ -(|a| \cdot b) & a < 0, b > 0 \\ -(a \cdot |b|) & a > 0, b < 0 \\ |a| \cdot |b| & a < 0, b < 0 \end{cases} \end{aligned}$$

A definição de inverso – para que possamos operar divisões – é

$$a^{-1} = \begin{cases} \sup\left\{\dfrac{1}{a^{(2n+1)}} \ : \ n \geq 0\right\} & a > 0 \\ -|a|^{-1} & a < 0 \end{cases}$$

O Teorema 15.20 nos garante que o que construímos foi de fato o corpo dos números Reais.

Teorema 15.20. *Todos os corpos ordenados completos são isomorfos.*

15.6 e é irracional

Já mostramos a irracionalidade de ϕ e de $\sqrt{k}$, quando k não é quadrado perfeito. Tratamos agora de e. Esta seção traz uma demonstração, elaborada por Henry Cohn, de que a expansão de e em fração contínua é de fato $[2; 1, 2, 1, 1, 4, 1, 1, 6, \ldots]$, e com isso ganhamos também a prova de que e é irracional, e de que não é quadrático (porque a sequencia não é periódica). Após esta, apresentamos outra demonstração, de Fourier, sem o uso de frações contínuas, e mais curta, mas que não leva à irracionalidade de e^2.

15.6.1 Demonstração de Cohn, com frações contínuas

A demonstração de Henry Cohn[7] consiste em provar, de maneira engenhosa, que a expansàо em fração contínua de e é infinita.

Primeiro observe que

$$[1;0,1,1,2,1,1,4,1,1,6,1,1,8,\ldots,1,1,2n,\ldots] = 1 + \cfrac{1}{0 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \ddots}}}},$$

é o mesmo que

$$[2;1,2,1,1,4,1,1,6,1,1,8,\ldots,1,1,2n,\ldots] = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}}}},$$

A primeira fração periódica não segue o padrão que impusemos, porque tem um coeficiente zero, mas ela pode ser descrita mais facilmente por relações de recorrência – por isso demonstraremos que ela é a expansão de e em fração contínua.

Além disso, observe que há um padrão nos coeficientes: eles são descritos por uma relação de recorrencia de ordem 3: $e = [1;0,1,\ \ 1,2,1,\ \ 1,4,1,\ \ \ldots]$. logo os coeficientes são

$$\begin{aligned} a_{3i} &= 1 \\ a_{3i+1} &= 2i \\ a_{3i+2} &= 1 \end{aligned}$$

Observamos os convergentes da fração contínua

i	0	1	2	3	4	5	6	7	8	9
p_i	1	1	2	3	8	11	19	87	106	193
q_i	1	0	1	1	3	4	7	32	39	71

[7] Henry Cohn (), Americano.

e os descrevermos também como relação de recorrência:

$$\begin{aligned} p_{3n} &= p_{3n-1} + p_{3n-2} & q_{3n} &= q_{3n-1} + q_{3n-2} \\ p_{3_n+1} &= 2np_{3n} + p_{3n-1} & q_{3n+1} &= 2nq_{3n} + q_{3n-1} \\ p_{3n+2} &= p_{3n+1} + p_{3n} & q_{3n+2} &= q_{3n+1} + q_{3n} \end{aligned}$$

Note que a sequência é descrita com três equações para p e três para q. Quando demonstrarmos propriedades desta sequência, faremos uma afirmação para cada um dos três casos $(3n, 3n+1, 3n+2)$.
Agora definimos três sequências, A_k, B_k e C_k, cada uma definida por uma integral:

$$\begin{aligned} A_n &= \int_0^1 \frac{x^n(x-1)^n}{n!} e^x dx \\ B_n &= \int_0^1 \frac{x^{n+1}(x-1)^n}{n!} e^x dx \\ C_n &= \int_0^1 \frac{x^n(x-1)^{n+1}}{n!} e^x dx \end{aligned}$$

É fácil verificar que A_n, B_n e C_n tendem a zero quando $n \to \infty$.
Com o Lema 15.4 queremos identificar três sequências da forma $q_n e - p_n$, que mais adiante usaremos. Note que, como mencionamos anteriormente, separamos em casos $3n$, $3n+1$ e $3n+2$.

Lema 15.4. *Para todo n natural,*

$$\begin{aligned} A_n &= q_{3n}e - p_{3n} \\ B_n &= p_{3n+1} - q_{3n+1}e \\ C_n &= p_{3n+2} - q_{3n+2}e \end{aligned}$$

Demonstração. Só precisamos mostrar que valem as condições iniciais

$$\begin{aligned} A_0 &= e - 1, \\ B_0 &= 1, \\ C_0 &= 2 - e, \end{aligned}$$

e que

$$A_n = -B_{n-1} - C_{n-1} \tag{15.1}$$
$$B_n = -2nA_n + C_{n-1} \tag{15.2}$$
$$C_n = B_n - A_n \tag{15.3}$$

As condições iniciais podem ser verificadas observando que, substituindo

$n = 0$ nas integrais, a relação de recorrência é satisfeita:

$$\begin{aligned} A_0 &= q_{3(0)}e - p_{3(0)} && = q_0 e - p_0 = e - 1 \\ B_0 &= p_{3(0)+1} - q_{3(0)+1}e && = p_1 - q_1 e = 1 \\ C_0 &= p_{3(0)+2} - q_{3(0)+2}e && = p_2 - q_2 e = 2 - e \end{aligned}$$

Para mostrar que 15.1 vale, basta integrar os dois lados de

$$\frac{x^n(x-1)^n}{n!}e^x + \frac{x^n(x-1)^{n-1}}{(n-1)!}e^x + \frac{x^{n-1}(x-1)^n}{(n-1)!}e^x = \frac{d}{dx}\left(\frac{x^n(x-1)^n}{n!}e^x\right).$$

Para 15.2, integre também os dois lados da equação:

$$\frac{x^{n+1}(x-1)^n}{n!}e^x + \frac{x^n(x-1)^{n-1}}{(n-1)!}e^x + \frac{x^{n-1}(x-1)^n}{(n-1)!}e^x = \frac{d}{dx}\left(\frac{x^n(x-1)^{n+1}}{n!}e^x\right).$$

Já 15.3 pode ser verificada trivialmente. □

Teorema 15.21.

$$e = [1; 0, 1, 1, 2, 1, 1, 4, 1, 1, 6, \ldots, 1, 1, 2n, \ldots]$$

Demonstração. Claramente, A_n, B_n e C_n tendem a zero quando $n \to \infty$. Observando o enunciado do Lema 15.4, isto significa que

$$\lim_{i\to\infty}(q_i e - p_i) = 0.$$

Como $q_i \geq 1$ e $i \geq 2$, temos

$$e = \lim_{i\to\infty}\frac{p_i}{q_i}.$$ □

Como a fração contínua de e é infinita, concluímos que e não é racional. A fração contínia de e também não é periódica, portanto e não é raiz de euqação quadrática, e concluímos que e^2 *também não é racional*.

15.6.2 Demonstração de Fourier, sem frações contínuas

A demonstração da irracionalidade de e com frações contínuas é interessante, e nos dá também a irracionalidade de e^2. Agora apresentamos, para comparação, uma demonstração mais curta – dada por Fourier[8] – da irracionalidade de e.

[8] Jean-Baptiste Joseph Fourier (1768-1830), Francês.

(Prova da irracionalidade de e, de Fourier). Partimos de

$$e = \sum_{k=0}^{\infty} \frac{1}{k!}.$$

Suponha que e seja racional: $e = p/q$, com $p, q \in \mathbb{N}$. Então

$$\begin{aligned} e = \frac{p}{q} &= \sum_{k=0}^{\infty} \frac{1}{k!} \\ q!\frac{p}{q} &= \sum_{k=0}^{\infty} \frac{q!}{k!} \\ (q-1)!p &= \sum_{k=0}^{\infty} \frac{q!}{k!} \\ &= \underbrace{\sum_{k=0}^{q} \frac{q!}{k!}}_{A} + \underbrace{\sum_{k=q+1}^{\infty} \frac{q!}{k!}}_{B}. \end{aligned}$$

O lado esquerdo, $(q-1)!p$, é inteiro, portanto o lado direito deve ser também. Mas A é claramente inteiro, porque

$$\begin{aligned} A &= \frac{q!}{1} + \frac{q!}{2} + \cdots \frac{q!}{q!} \\ &= q! + [3 \cdot 4 \cdot q] + \cdots + [(q-2)(q-1)q] + [(q-1) \cdot q] + 1. \end{aligned}$$

Assim, B deve também ser inteiro. Mas mostraremos que (i) $B > 0$, e (ii) $B < 1$, de forma que B não pode ser inteiro, levando a uma contradição.

Para (i), note que os termos de B são todos maiores que zero. Para (ii),

basta calcular

$$\begin{aligned}
B &= \sum_{k=q+1}^{\infty} \frac{q!}{k!} \\
&= \sum_{k=q+1}^{\infty} \frac{1}{(q+1)(q+1)\cdots k} \\
&< \sum_{k=q+1}^{\infty} \frac{1}{(q+1)^k} \\
&< \sum_{k=1}^{\infty} \frac{1}{(q+1)^k} \\
&= \frac{1}{q+1}\left(\frac{1}{1-\frac{1}{q+1}}\right) \\
&= \frac{1}{q} \\
&< 1.
\end{aligned}$$

□

15.7 π é irracional

Uma vez que são conhecidos muitos dos primeiros dígitos de π, também conhecemos muitos dos primeiros coeficientes de sua expansão em fração contínua,

$$\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, \dots]$$

No entanto, não conhecemos forma fechada para estes coeficientes – o que é o mesmo que dizer que não conhecemos uma descrição completa da expansão de π em frações contínuas simples, *da forma como as definimos*. No entanto, há várias expansões de π em frações contínuas onde as regras de formação que impusemos são quebradas. Algumas delas são

$$\pi = \cfrac{4}{1+\cfrac{1^2}{3+\cfrac{2^2}{5+\cfrac{3^2}{7+\cfrac{4^2}{9+\ddots}}}}} \qquad \pi = \cfrac{4}{1+\cfrac{1^2}{2+\cfrac{3^2}{2+\cfrac{5^2}{2+\cfrac{7^2}{2+\ddots}}}}}$$

$$\pi = 3+\cfrac{1}{6+\cfrac{3^2}{6+\cfrac{5^2}{6+\cfrac{7^2}{6+\cfrac{9^2}{6+\ddots}}}}} \qquad \frac{\pi}{2} = 1+\cfrac{1}{1+\cfrac{1}{1/2+\cfrac{1}{1/3+\cfrac{1}{1/4+\ddots}}}}$$

Nesta seção não derivaremos uma fração contínua para π; ao invés disso, obteremos a expansão de $\tan(x)$ em fração contínua, e dela concluiremos que π^2 e π são irracionais – esta é em essência a mesma demonstração dada por Johann Lambert[9] em 1761.

Lema 15.5. *Se*

$$x = \cfrac{a_1}{b_1+\cfrac{a_2}{b_2+\cfrac{a_3}{b_3+\cfrac{a_4}{b_4+\ddots}}}}$$

e, para i *maior que algum* N *suficientemente grande sempre for verdade que* $|a_i| < |b_i|$*, então* x *é irracional.*

Lema 15.6.

$$\tan(x) = \cfrac{x}{1-\cfrac{x^2}{3-\cfrac{x^2}{5-\ddots}}}$$

Teorema 15.22. *π é irracional.*

Demonstração. Suponha que π é racional. Então $\pi/4$ também é:

$$\frac{\pi}{4} = \frac{a}{b}, \quad a, b \in \mathbb{Z}.$$

[9] Johann Heinrich Lambert (1728-1777), Suíço.

Substituimos $\pi/4$ por a/b na expansão em fração contínua de $\tan(\pi/4)$:

$$\tan\left(\frac{\pi}{4}\right) = \tan\left(\frac{a}{b}\right).$$

Como $\tan(\pi/4) = 1$, podemos igualar 1 à expansão em fração contínua de $\tan(a/b)$:

$$\begin{aligned} 1 &= \cfrac{\frac{a}{b}}{1 - \cfrac{\frac{a^2}{b^2}}{3 - \cfrac{\frac{a^2}{b^2}}{5 - \cfrac{\frac{a^2}{b^2}}{7 - \ddots}}}} \\ &= \cfrac{a}{b - \cfrac{a^2}{3b - \cfrac{a^2}{5b - \cfrac{a^2}{7b - \ddots}}}} \end{aligned}$$

Notamos que os a_i são constantes (são todos iguais a a^2), mas os b_i crescem, e eventualmente, $kb_i > a^2 + 1$. Isto significa que a expansão é irracional – o que é absurdo, já que este é o número um. □

Como π é a razão entre o comprimento e o diâmetro de qualquer circunferência, resulta que um dos dois (diâmetro ou circunferência) necessariamente será irracional. Ao traçar uma circunferência com raio (e diâmetro) racional, estamos desenhando uma linha de comprimento irracional!

15.8 ϕ é irracional

O valor ϕ, também chamado de *razão áurea*, é definido como segue. Para quaisquer números reais, a, b, com $a > b > 0$, se

$$\frac{a}{b} = \frac{a+b}{a}.$$

então $\phi = a/b$.

Isto implica que

$$\begin{aligned}\phi &= \frac{a+b}{a}\\ &= \frac{a}{a}+\frac{b}{a}\\ &= 1+\frac{b}{a}\\ &= 1+\frac{1}{\phi},\end{aligned}$$

e ϕ deve ser a raiz positiva de $\phi = 1 + 1/\phi$, ou seja, a raiz positiva de

$$\phi^2 - \phi - 1 = 0.$$

Teorema 15.23. *ϕ, solução da equação $\phi^2 - \phi - 1 = 0$, é irracional.*

Demonstração. O fato de $\phi = 1 + 1/\phi$ já nos dá a expansão em fração contínua, $\phi = [1; 1, 1, 1, \cdots]$, que é infinita (e periódica!). □

Há algumas outras demonstrações muito curtas e simples de que ϕ é irracional. Estas demonstrações não envolvem usar frações contínuas ou qualquer ferramenta de Cálculo.

Demonstração. Suponha que $\phi = a/b$, com $a, b \in \mathbb{Z}$, seja raiz positiva da equação. Então

$$\begin{aligned}\left(\frac{p}{q}\right)^2 - \frac{p}{q} - 1 &= 0\\ \left(\frac{p}{q}\right)^2 - \frac{p}{q} &= 1\\ p^2 - pq &= q^2\\ p(p-q) &= q^2,\end{aligned}$$

o que implica que $p|q^2$, e poratnto p e q tem um fator comum. Como presumimos que isto não acontece, somos obrigados a admitir que p seja 1. Mas isso implicaria que

$$q = \frac{1}{\phi},$$

que não é inteiro. □

Como ϕ é a solução positiva de $\phi^2 - \phi - 1 = 0$, então

$$\phi = \frac{1+\sqrt{5}}{2}.$$

Isto pode ser usado em outra demonstração da irracionalidade de ϕ. Esta demonstração presume que já se estabeleceu que $\sqrt{5} \notin \mathbb{Q}$.

Demonstração. Suponha que

$$\frac{1+\sqrt{5}}{2} \in \mathbb{Q}.$$

Então

$$2\left(\frac{1+\sqrt{5}}{2}\right) - 1 = \sqrt{5},$$

mas então obtivemos um irracional ($\sqrt{5}$) simplesmente realizando uma divisão e uma subtração em um racional – o que é impossível. □

15.9 Exercícios

Ex. 331 — Represente $2/3$, $20/3$, $11/13$ e $21/13$ como frações contínuas.

Ex. 332 — Expanda as frações contínuas como números racionais: $[0;1,2,3]$, $[0;3,2,1]$, $[0;10,10,10]$, $[1;9,9]$.

Ex. 333 — Determine as expansões de $\sqrt{11}$ e $\sqrt{12}$ como frações contínuas.

Ex. 334 — Obtenha a expansão de $\sqrt{5}$ em fração contínua, e conclua que $\sqrt{5}$ é irracional.

Ex. 335 — Determine a expansão em fração contínua de $(b+\sqrt{b^2-4ac})/2a$.

Ex. 336 — Seja $x \in \mathbb{R}$ positivo, e a_1, b_1, a_2, b_2 tais que $a_2b_1 - a_1b_2 = 1$, e

$$\frac{a_1}{b_1} < x < \frac{a_2}{b_2}.$$

Prove que uma das duas frações deve ser convergente na expansão de x.

Ex. 337 — Seja $x = [x_0; x_1, x_2, \dots]$ um número irracional, e sejam $y_1, y_2, \dots$ uma sequência de inteiros positivos. Prove que

$$\lim_{k\to\infty} [x_0; x_1, \dots, x_k, y_1, y_2, \dots] = x$$

Ex. 338 — Seja A um número representável por fração contínua periódica. Prove que A é da forma

$$\frac{a+\sqrt{b}}{c},$$

onde $a, b, c \in \mathbb{Z}$ e b não é quadrado perfeito.

Ex. 339 — Seja

$$A = \frac{a + \sqrt{b}}{c},$$

onde $a, b, c \in \mathbb{Z}$ e b não é quadrado perfeito. Prove que A pode ser escrito como fração contínua periódica.

Ex. 340 — Dado um intervalo, como determinar o racional dentro dele que tenha o menor numerador e o menor denominador? (Dica: represente as extremidades como frações contínuas).

Ex. 341 — Seja $x = [x_0; x_1, x_2, \dots]$

$$P_k = \begin{pmatrix} x_0 & -1 & 0 & \cdots & 0 & 0 \\ 1 & x_1 & -1 & & & 0 \\ 0 & 1 & \ddots & & & 0 \\ \vdots & & & & & \vdots \\ 0 & & & & x_{n-1} & -1 \\ 0 & 0 & 0 & \cdots & 1 & x_k \end{pmatrix}$$

e Q_k a matriz obtida removendo a primeira linha e aprimeira coluna de P_k Prove que $p_k = \det P_k$, e que $q_k = \det Q_k$.

Ex. 342 — Encontre um contraexemplo para a recíproca do Lema 15.3.

Ex. 343 — É possível construir um espaço métrico a partir de $\mathbb{Q}^2$ usando a distância de Manhattan,

$$d\Big((x_1, y_1), (x_2, y_2) \Big) = |x_1 - x_2| + |y_1 - y_2|.$$

Para cada vetor $v = (x, y)$, com $x, y \in \mathbb{Q}$, é possível definir uma sequência

$$s_n^v = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix},$$

com $a, b, c \in \mathbb{Q}$. Determine precisamente quando s_n^v é de Cauchy (para quais noções de distância, e quais, a, b, c, x, y).

Ex. 344 — O número $0,999\cdots$, onde a quantidade de noves após a vírgula

é infinita, é o número um. Como consequência,

$$1,999\cdots = 2,$$
$$2,5999\cdots = 2,6.$$

Prove, usando a construção de reais que demos neste Capítulo, que $0,999\cdots = 1$.

Capítulo 16

Régua e compasso: o corpo dos números construtíveis

As regras para construções com régua e compasso estão intimamente relacionadas aos postulados da Geometria Euclideana – em particular, os dois primeiros, que não tratam de angulos.

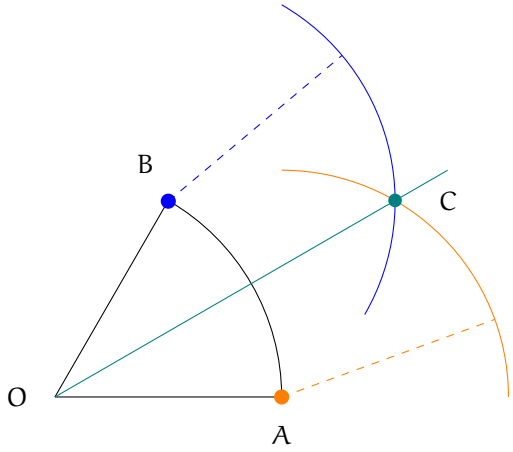
Definição 16.1 (construção com régua e compasso)**.** *Uma* ***construção clássica com régua e compasso*** *deve ser realizada a partir de dois pontos iniciais distintos, e usando apenas as operações a seguir, com uma régua e um compasso.*

- *com a régua, retas podem ser traçadas passando por dois pontos;*
- *dado um ponto e uma distância, um círculo pode ser traçado com o compasso;*
- *a partir de duas retas, ou dois círculos, ou uma reta e um círculo, é possível indentificar os pontos de interseção, e portanto aumentar o conjunto de pontos.*

Podem ser arbitrariamente grandes o comprimento da régua e a abertura do compasso, e a régua não pode ter marcações. ◀

Os gregos conseguiram determinar como, usando apenas régua e compasso, realizar as quatro operações aritméticas básicas, além de diversas outras operações – extrair raízes quadradas, obter a bisecção de ângulos, criar um quadrado com o dobro de uma dada área, criar um quadrado com o mesmo volume de um polígono dado, e construir polígonos com alguns números específicos de lados. Havia, no entanto, construções que os gregos não conseguiam realizar, e cujas demonstrações de impossibilidade só foram obtidas muito mais tarde.

Para um exemplo simples de construção com régua e compasso, examinamos a bisecção de um ângulo. São dadas duas retas não paralelas que se interceptam em um ponto O. Marcamos dois pontos, um em cada reta, e a uma mesma distancia de O. Nomeamos os pontos A e B. Desenhamos dois círculos, um com centro em A, e um com centro em B; o raio deve ser maior que a distância de A até B. Estes dois círculos se interceptam em dois pontos; tomamos um deles, C, e a reta OC é a bissetriz do ângulo dado.



16.1 Números construtíveis

Embora seja possível trabalhar com "pontos" construtíveis no plano, podemos usar, como já fizemos anteriormente, o plano complexo. Assim, o ponto (a, b) corresponde ao número complexo $a + bi$.
Definimos, portanto, número construtível. Partimos da existencia de dois pontos diferentes, e construímos outros a partir deles. É necessário agora formalizar o que consideramos "construção com régua e compasso":

Definição 16.2 (número construtível)**.** *Denotando o número complexo* $a + bi$ *por* (a, b)*, os* ***números construtíveis*** *correspondem aos pontos a seguir.*

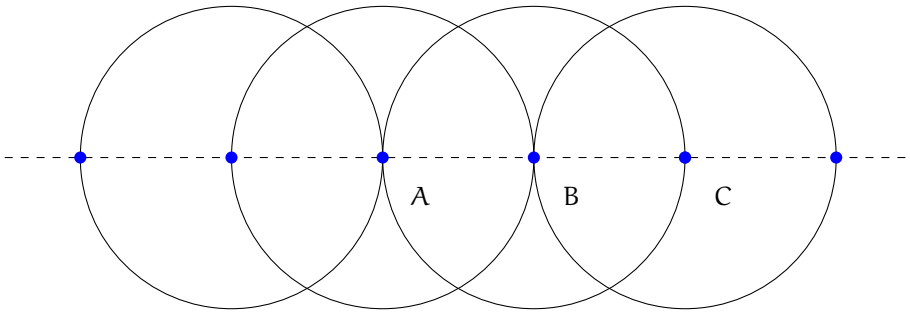
- *Os pontos* $(0, 0)$ *e* $(1, 0)$ *são construtíveis.*
- *Se* P *e* Q *são dois pontos construtíveis, então a reta passando por* P *e* Q *também é (e evidentemente, o segmento indo de* P *até* Q *também).*
- *Se* P *e* Q *são construtíveis, então a circunferência com centro em* P *e raio* PQ *é construtível (porque podemos posicionar a ponta seca do compasso em* P *e a outra ponta em* Q*).*
- *Os pontos de interseção de dois objetos construtíveis. são construtíveis.* ◀

Determinaremos agora quais números são construtíveis. Gradualmente identificaremos conjuntos numéricos. O primeiro conjunto de números construtíveis será o dos inteiros ($\mathbb{Z}$) – os pontos inteiros no eixo real.

Assim, verificamos a seguir que podemos identificar os eixos real e imaginário, e construir todos os pontos inteiros nesses eixos.

Lema 16.1. *O conjunto $\mathbb{Z}$ é construtível.*

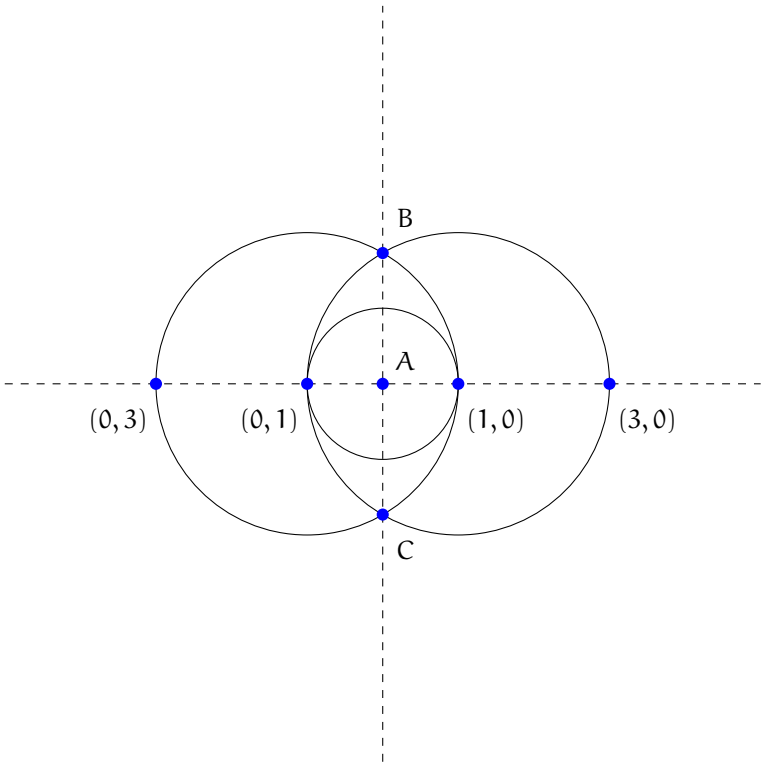
Demonstração. Podemos construir pontos equidistantes no eixo real tendo dois pontos iniciais A e B; escolhemos A como origem. Criamos inicialmente um círculo com centro em A e raio igual a d, a distancia entre A e B. Depois, criamos outro círculo com centro em B, e raio d. Agora, os pontos A e B determinam uma reta, que será o eixo real. Os outros pontos podem ser obtidos facilmente – por exemplo, C é a interseção do círculo com centro em B com a reta AB.



Com isso provamos que os números da forma $(k, 0)$, com $k \in \mathbb{Z}$, são construtíveis (e portanto $\mathbb{Z}$ é construtível). □

Teorema 16.1. *Os números da forma $(0, k)$, com $k \in \mathbb{Z}$ são construtíveis.*

Demonstração. Para traçar o eixo imaginário, traçamos uma reta perpendicular a AB, passando por A. Para isso, desenhamos um círculo com centro em A e raio 1. Depois, traçamos dous círculos, com centro em $(1, 0)$ e $(-1, 0)$, com raio 2. As interseções destes círculos, nos pontos B e C, determinam uma reta perpendicular a AB.

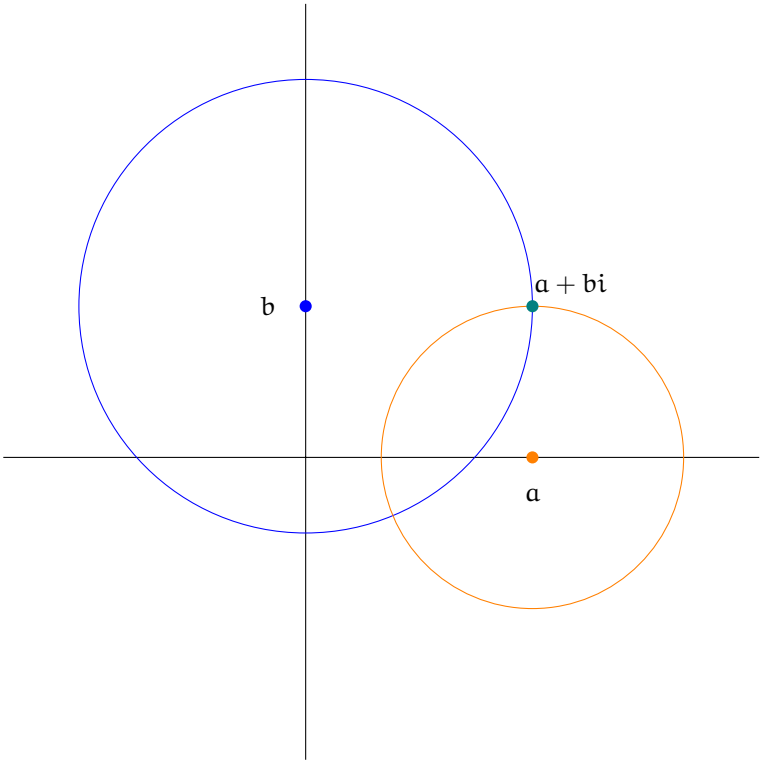


Tendo a origem, o eixo imaginário, e número $1 + 0i$ (que é o ponto $(1, 0)$) é possível construir os pontos $(0, y)$, com $y \in \mathbb{Z}$. □

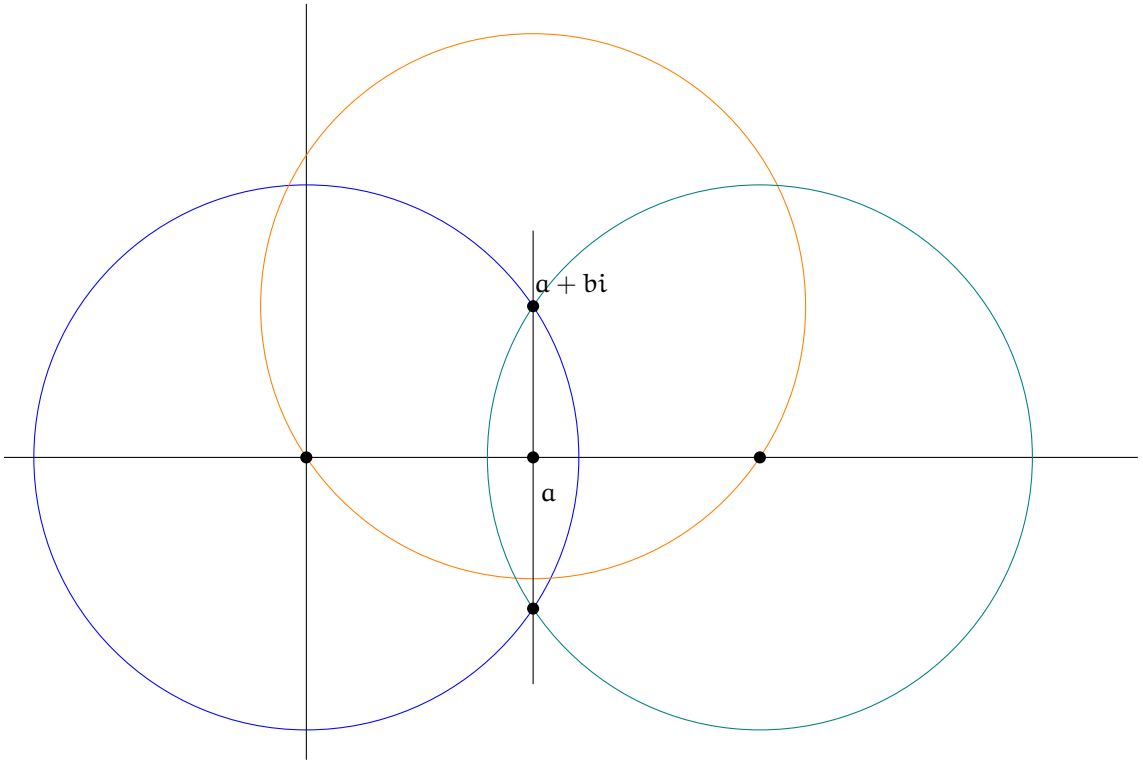
Naturalmente, o próximo passo é mostrar como combinar os números que já temos, a fim de obter $a + bi$ a partir de a e de bi.

Lema 16.2. $a+bi$ *e* $a-bi$ *podem ser construídos se e somente se os pontos* a *e* bi *podem ser construídos.*

Demonstração. Se $a+0i$ e $0+bi$ são construtíveis, então podemos criar dois círculos, um com raio b no ponto a e um com raio a no ponto bi. Um dos dois pontos onde estes círculos se encontram é $a + bi$.



A partir do ponto $a + bi$, podemos baixar perpendiculares nos dois eixos. A figura a seguir ilustra a obtenção de a a partir de $a + bi$.



Primeiro, desenha-se o círculo com centro em $a+bi$ e passando pela origem. Depois, com o mesmo raio, desenham-se dois círculos, nos dois pontos em que o primeiro círculo intercepta o eixo real. Basta agora traçar a perpendicular, que passa pelasinterseções dos dois últimos círculos.
Notamos que esta construção também nos dá $a - bi$. □

A técnica usada é útil para obter o conjugado de um número.

Corolário 16.1. *Se z é construtível, $\bar{z}$ também é.*

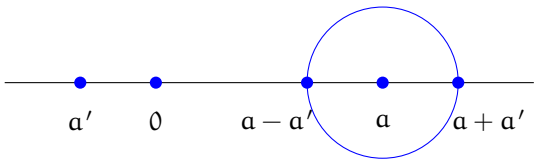
Demonstração. Se $z = a + bi$, basta baixar perpendiculares para obter os pontos $(a, 0)$ e $(0, b)$, e assim construir $a - bi$. □

Finalmente, tratamos das operações de soma e multiplicação, com suas inversas. Começamos pela soma.

Lema 16.3. *Dados dois complexos x e y, é possível construir $x + y$ e $x - y$ (o que implica que os inteiros Gaussianos são construtíveis).*

Demonstração. Queremos somar dois complexos, $x = a + bi$ e $y = a' + b'i$. Mostramos que o enunciado vale no eixo dos reais – o que significa que também vale no eixo imaginário, e como a soma de complexos se dá comando

os componentes real e imaginário separadamente, isto bastará. Geometricamente, se pudermos somar as coordenadas separadamente nos dois eixos, $a+a'$ e $b+b'$, o Lema 16.2[1] garante que a partir dessas novas coordenadas podemos construir $(a+a')+(b+b')i$.
Dados a e a' no eixo real, temos a distância da origem até a'. Criamos um círculo centrado em a com raio igual a essa distância, e um dos pontos de interseção do círculo com o eixo é $a+a'$; o outro é $a-a'$.

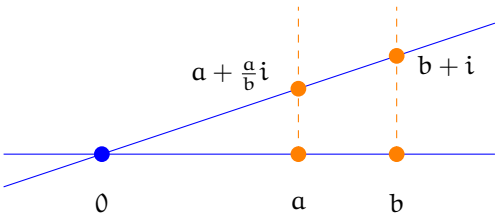


□

Passamos à multiplicação.

Lema 16.4. *Dados dois complexos x e y, é possível construir xy e, quando $y \neq 0$, x/y.*

Demonstração. Tendo a e a' no eixo real, é possível construir $b+i$. Traçamos uma reta da origem até $a'+i$; depois, traçamos uma reta perpendicular a a, e marcamos o ponto onde ela se intercepta com a reta traçada anteriormente.



O ponto obtido é $a+(a/b)i$, e pelo Lema 16.2, é possível obter $(a/b)i$ e a/b. O procedimento inverso pode ser usado para obter ab a partir de a e b. □

Teorema 16.2. *Os números construtíveis formam um corpo.*

Demonstração. Segue dos lemas anteriores. As quatro operações podem ser realizadas, e valem associatividade, comutatividade e distributividade como usualmente. Há elemento neutro para adição (a origem); e elemento neutro para multiplicação: $(1,0)$, ou $1+0i$. □

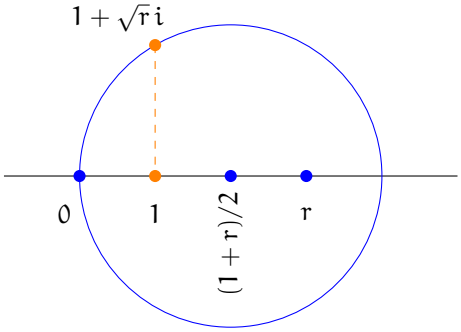
Corolário 16.2. *$\mathbb{Q}$ e $\mathbb{Q}[i]$ são construtíveis.*

[1] **Lema 16.2:** $a+bi$ e $a-bi$ podem ser construídos se e somente se os pontos a e bi podem ser construídos.

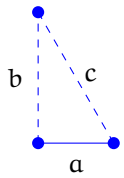
O conjunto $\mathcal{C}$, além de ser um corpo, tem outra propriedade – é fechado para a extração de raízes quadradas.

Teorema 16.3. *Se* $x^2 \in \mathcal{C}$*, então* $x \in \mathcal{C}$*.*

Demonstração. Provamos que, se $r \in \mathcal{C}$, então $\sqrt{r} \in \mathcal{C}$.
Trace um círculo com centro em $(1+r)/2$, e raio também $(1+r)/2$.



Agora trace uma perpendicular ao eixo real, passando pelo um. Ela interceptará o círculo nos pontos $1 \pm \sqrt{r}\,i$. Isto pode ser facilmente verificado usando o Teorema de Pitágoras.



$$a = \frac{r}{2} + \frac{1}{2}$$
$$c = \frac{1+r}{2}$$

e $b = \sqrt{c^2 - a^2}$ resulta em $\sqrt{r}$. □

É interessante que, sendo possível calcular $\sqrt{x}$, pode-se calcular $\sqrt[2^k]{x}$, para todo $k \in \mathbb{N}$, já que

$$\sqrt[2^k]{x} = \sqrt{\sqrt[2^{k-1}]{x}}.$$

O fato de podermos extrair raízes quadradas implica que $\mathcal{C}$ é superconjunto *estrito* de $\mathbb{Q}[i]$. E, como os números construídos são todos complexos,

$$\mathbb{Q}[i] \subset \mathcal{C} \subseteq \mathbb{C}.$$

Os números que conseguimos construir são, portanto, da forma $a + bi$, onde a e b são da forma $r\sqrt[2^k]{s}$, com $r, s \in \mathbb{Q}$ e $k \in \mathbb{N}$.

Na próxima seção mostraremos que a segunda inclusão também é estrita ($\mathcal{C} \subset \mathbb{C}$).

16.2 Todos os números construtíveis

As construções na Seção anterior são interessantes e contribuem para o desenvolvimento de uma intuição relacionada aos números construtíveis. No entanto, da maneira como foram colocadas, elas não permitiram determinar o que *não* pode ser construído com régua e compasso. O Teorema 16.4 determina exatamente quais números podem ser construídos.

Teorema 16.4. *Seja* K *o conjunto dos números da forma* $a + bi$*, onde* a *e* b *são da forma* $r\sqrt[2^q]{s}$*, com* $r, s \in \mathbb{Q}$ *e* $q \in \mathbb{N}$*.*

Os <u>únicos</u> números possíveis construtíveis são da forma $\frac{a}{b} + \frac{c}{d}i$*, onde* a, b, c, d *estão em* K*.*

Demonstração. O conjunto $\mathcal{C}$ contém, além de 1 e i, interseções entre objetos, que são sempre retas ou circunferências.

A interseção de duas retas passando por pontos em K resulta de um sistema com duas equações lineares, ambas com coeficientes em K, e portanto é obtido usando as quatro operações básicas, para as quais K é fechado.

Consideramos agora a interseção de duas circunferências construídas com régua e compasso. Para cada uma. o centro é um número construtível, e um ponto da borda (um dos pontos por onde o compasso passou) é também construtível. O raio, que é subtração de dois números da forma $a + bi$, com coeficientes em K, também o será.

As interseções entre as duas circunferências serão o resultado do sistema

$$\begin{aligned}(x - a)^2 + (y - b)^2 &= e\\ (x - c)^2 + (y - d)^2 &= f,\end{aligned}$$

com todos os coeficientes e termos constantes em K. Se expandirmos os termos elevados ao quadradoe subtrairmos a segunda equação da primeira, teremos

$$2(c - a)x + 2(d - b)y = e - f - a^2 - b^2 + c^2 + d^2,$$

que é a equação de uma reta com todos os coeficientes em K. Assim, o caso de duas circunferências é o mesmo caso de uma circunferência com uma reta.

Finalmente, o caso da interseção de uma reta com uma circunferência é

simples: o resultado será a solução de um sistema da forma

$$ax + by = e,$$
$$(x - c)^2 + (y - d)^2 = f,$$

e o resultado será obtido usando as quatro operações elementares e raiz quadrada – todas operações para as quais K é fechado.
Assim, $\mathcal{C} = K$. □

Corolário 16.3. *Raízes cúbicas, quintas, de grau ímpar ou, de maneira geral, com grau diferente de potência de dois não são construtíveis, e* $\mathcal{C} \subset \mathbb{C}$ *(inclusão estrita: os conjuntos não são iguais).*

16.3 Alguns problemas impossíveis

Algumas construções geométricas dependem do uso de comprimentos dados por números não construtíveis, por isso não são possíveis de realizar com régua e compasso, *usando as regrasque determinamos no início do Capítulo*.

- **Duplicação do volume de um cubo**

  A partir de um cubo, o objetivo é construir outro, com o dobro do volume.

  Considere um cubo com lado unitário. O cubo com o dobro do volume teria que ser construído de forma que seu volume seja 2, e portanto com lado de comprimento $\sqrt[3]{2}$, que não é construtível.

- **Trisecção de um ângulo**

  A trisecção de um ângulo α com régua e compasso consiste em obter pontos que determinem duas retas formando um ângulo $\alpha/3$.

  Seja α igual a 60^o, ou $\pi/3$. A trisecção deste angulo nos daria ângulos de 20^o, ou $\pi/9$. Mas se este ângulo pudesse ser construído, a distância dad pelo seu cosseno também o seria (pela definição de cosseno, basta baixar um aperpendicular). No entanto, $\cos \pi/9$ é raiz de

  $$8x^3 - 6x - 1,$$

  e não há[2] polinômio de menor grau, com coeficientes racionais, do qual ele seja raiz.

[2]Não estamos demonstrando, apenas comentando. Para um argumento com rigor, teríamos que provar que de fato este polinômio não é redutível em $\mathbb{Q}$ – o que fica fora do escopo deste texto.

- **Quadratura do círculo**

  Obter a "quadratura de um círculo" é, dado um círculo, construir um quadrado com a mesma área.

  Considere um círculo com raio unitário: sua área é π. Um quadrado com área π precisaria ter lado com comprimento igual a $\sqrt{\pi}$, que não é construtível.

Exercícios

Ex. 345 — Dados dois pontos A e B, mostre como construir um quadrado tendo como um dos lados o segmento AB.

Ex. 346 — Dados dois pontos A e B, mostre como construir um triângulo equilátero tendo como um dos lados o segmento AB.

Ex. 347 — Prove que há infinitos números construtíveis

a) na borda de uma circunferência construtível, e

b) no interior de uma circunferência construtível.

Ex. 348 — Números algébricos são raizes de equações polinomiais com coeficientes racionais. Por exemplo, $1 + 2i$ é algébrico, porque é raiz da equação $x^4 - 4x^3 + 10x^2 - 12x + 5 = 0$; A razão áurea é um número algébrico, porque é raiz da equação $x^2 - x - 1 = 0$; já π não é algébrico, porque não é raiz de qualquer equação linear com coeficientes racionais. Denote o conjunto dos números algébricos por $\mathcal{A}$. Qual a relação entre $\mathcal{A}$ e $\mathcal{C}$? Um está contido no outro?

Ex. 349 — Dados os pontos $0+0i$ e $1+0i$, como é possível construir o ponto $\cos(\pi/6) + \sin(\pi/6)i$?

Ex. 350 — Se for possível usar uma régua com dois pontos diferentes marcados, as construções realizadas não são mais as clássicas construções Euclideanas com régua e compasso. Mostre que, com uma régua dessas, é possível realizar a trisecção de qualquer ângulo.

Apêndices

Apêndice A

Dicas e Respostas

Resp. (Ex. 10) — Em (a), $k = 3$, e em (b), $k = 4$.

Resp. (Ex. 11) — (Dica) As duas equações a seguir são equivalentes.

$$a^2 + b^2 = c^2$$
$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$$

Resp. (Ex. 17) — Duas matrizes invertíveis podem ser somadas resultando em uma singular. O conjunto não seria fechado para soma.

Resp. (Ex. 18) — Um polinômio "$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$" significa

$$\begin{aligned}
&\text{“ } a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \text{ ”} \\
=&a_n \otimes \underbrace{x \otimes x \otimes x \cdots x}_{n \text{ vezes } x} \ \oplus \ a_{n-1} \otimes \underbrace{x \otimes x \otimes x \cdots x}_{n-1 \text{ vezes } x} \ \oplus \ \cdots \ \oplus \ a_0 \\
=&a_n + \underbrace{x + x + x \cdots x}_{n \text{ vezes } x} \ \oplus \ a_{n-1} + \underbrace{x + x + x \cdots x}_{n-1 \text{ vezes } x} \ \oplus \ \cdots \ \oplus \ a_0 \quad (\otimes \ \to \ +) \\
=&a_n + nx \ \oplus \ a_{n-1} + (n-1)x \ \oplus \ \cdots \ \oplus \ a_0 \\
=&\max\Big(a_n + nx, \ a_{n-1} + (n-1)x, \ \cdots, \ a_0\Big). \qquad (\oplus \ \to \ \max)
\end{aligned}$$

Resp. (Ex. 21) — Só haverá um símbolo a usar, e a quantidade dele é a quantidade representada (diferente do esquema apresentado no texto!) Note que, usando somente o dígito 1, ainda vale

$$n = \sum_{i=0}^{k} d_k 1^k.$$

Por exemplo, 111 é a representação de 3, porque

$$\begin{aligned} n &= 1 \cdot 1^2 + 1 \cdot 1^1 + 1 \cdot 1^0 \\ &= 1 + 1 + 1 \\ &= 3. \end{aligned}$$

Resp. (Ex. 24) — Veja o Exercício 23.

Resp. (Ex. 25) — (Dica) Escreva

$$\frac{1}{7} = \frac{a_1}{60} + \frac{a_2}{60^2} + \ldots + \frac{a_n}{60^n},$$

Simplifique o lado direito, de forma a manter 60^n no denominador.

Resp. (Ex. 43) — Escreva $n = 7q + r$, com $q \in \mathbb{Z}$ e $r < 7$. Depois escreva $7(4q^2) = 7k$; $7(7q^2 + 2q) + 1 = 7k + 1$; $7(7q^2 + 4q) + 1 = 7k + 4$, e observe que o resto de um quadrado dividido por 7 só pode ser $0, 1, 2$ ou 4...

Resp. (Ex. 45) — n inteiros positivos consecutivos são sempre divisíveis por n...

Resp. (Ex. 48) — (Dica) Se o racional é a/b, então divida b por a:

$$b = aq + r, \qquad 0 \leq r < a.$$

Base: se $r = 0$ então $a/b = 1/q$.
Siga com o passo, indução no numerador.

Resp. (Ex. 49) — (Dica) Seja $n \in \mathbb{N}$. Considere os números 1, 11, ..., $111\ldots1$ (n números) Divida cada um por n.

Resp. (Ex. 50) — A inversa de matriz 2×2 tem forma fechada bastante simples. Veja ali que será necessário que os números

$$\frac{a}{a^2 - b^2}, \quad \frac{b}{a^2 - b^2}$$

sejam inteiros.

Resp. (Ex. 54) — $ab - b^2$. Use as propriedades básicas do MDC.

Resp. (Ex. 56) — Descida infinita.

Resp. (Ex. 63) — Uma que evidentemente pode ser tentada é usando a fórmula de Euler-Binet (basta escrever os termos de maneira adequada). Outra possibilidade é usando a igualdade de Honsberger, e aplicando indução.

Resp. (Ex. 64) — Uma possível demonstração:
Por indução em n.

A base é trivial, com $n = 1$: $u_m \mid u_{m \cdot 1}$, que é o mesmo que dizer que $u_m \mid u_m$.

Para a hipótese, presuma que, para todo m, $u_m \mid u_{mj}$ para todo número menor j que n.

Agora, observando que o Lema 4.8 afirma que $u_{m(n+1)} = u_{mn+m}$,

$$u_{m(n+1)} = u_{m(n-1)}u_m + u_{mn}u_{m+1}.$$

Como $u_m \mid u_{mn}$, o lado direito é divisível por u_m, e $u_m \mid u_{m(n+1)}$.

Resp. (Ex. 66) — Lema de Honsberger não, e consequentemente o Teorema 4.16 não. O Lema 4.15 vale desde que os dois valores iniciais sejam coprimos.

Resp. (Ex. 77) — Use o Teorema 4.12.

Resp. (Ex. 82) — Fatore. Nenhum deles tem mais que três divisores primos distintos.

Resp. (Ex. 93) — Como $d' \mid a$, $d' \mid b$, então $d \mid d'$, portanto deve haver

$k \in X$ tal que $kd' = d$. Mas então

$$\lambda(d') \leq \lambda(kd') = \lambda(d).$$

Se d' também é máximo divisor comum, então $d' \mid d$, e pelo mesmo argumento, chega-se a $\lambda(d') = \lambda(d)$.

Resp. (Ex. 94) — (Dica) Função de valoração:

$$\nu\left(\sum_i a_i x^i\right) = \text{ menor } i \text{ tal que } a_i \neq 0.$$

Resp. (Ex. 95) — O algoritmo estendido de Euclides, usado para obter os coeficientes de Bézout, funciona em qualquer domínio Euclideano.

Resp. (Ex. 96) — $n^3 - 1 = (n-1)(n^2+n+1)$, e este produto é primo.

Resp. (Ex. 98) — Considere os casos $n = 3k+1$, $n = 3k+2$, e conclua que n só pode ser $3k$.

Resp. (Ex. 100) — Considere que (i) $2 \mid n!$, também que (ii) $n \mid n!$, e depois prove que (iii) $n! - 1 > n$. Evidentemente, (iv) $n! - 1 < n!$. Em seguida, veja que como $n!$ é par, então (v) $n! - 1$ é ímpar. Por isso, existe algum p tal que (vi) $p \mid n! - 1$, $p \neq 2$. Mas isso significa que (vii) $p < n!$, claro (porque divide $n! - 1$).

Se $p \leq n$, então $p \mid n!$ Mas isso implicaria em $p \mid n!$ e <u>também</u> em $p \mid n! - 1$, absurdo. Logo, (viii) $p > n$.

Com (vii) e (viii) o resultado é estabelecido.

Resp. (Ex. 101) — Primeira parte: Pelo pequeno teorema de Fermat, P divide $2^{p-1} - 1$, portanto

$$\begin{aligned} &p \mid 2^{p-1} - 1 \\ &p \mid 2(2^{p-1} - 1) && \text{(se divide } n\text{, divide } 2n\text{)} \\ &p \mid (2^p - 2). \end{aligned}$$

Então,

$$\begin{aligned} &p \mid 2^p + 1 \\ &p \mid (2^p + 1) - (2^p - 2) \\ &p \mid 3, \end{aligned}$$

e $p = 3$.

Resp. (Ex. 102) — Expanda a combinação em fatoriais, $\binom{p}{k} = p!/k!(p-k!)$. Isole $p!$. Use o Teorema de Euclides[17].

Resp. (Ex. 103) — Presuma $\sqrt[k]{n} = a/b$, com $\operatorname{mdc}(a, b) = 1$. O que acontece se $b > 1$?

Resp. (Ex. 105) — Suponha que $p < q$ são primos consecutivos, e que $p + q = 2t$. Então $t = (p + q/2)$, e claramente, $p < t < q$. Mas t, estando entre p e q, não pode ser primo, porque p e q são primos consecutivos.

Resp. (Ex. 106) —

$$\begin{aligned} \operatorname{mdc}\left(\frac{p+1}{2}, \frac{p\text{-}1}{2}\right) &= 2\operatorname{mdc}(p+1, p\text{-}1) \\ &= 2\operatorname{mdc}(p+1\text{-}(p\text{-}1), p\text{-}1) \\ &= 2\operatorname{mdc}(2, p\text{-}1) \\ &= \operatorname{mdc}\left(1, \frac{p\text{-}1}{2}\right) \\ &= 1. \end{aligned}$$

Resp. (Ex. 107) — Todo F_n deixa resto dois quanto dividido por 5, e são todos ímpares.

Resp. (Ex. 108) — Para F_0 e F_1 é evidente. Para outros, como terminam com dígito 7, não são quadrados (veja o Exercícios 23).

Resp. (Ex. 109) — Indução em n.

[17] **Lema 4.3 (de Euclides)**: Se p é primo e $p \mid ab$, então $p \mid a$ ou $p \mid b$.

Resp. (Ex. 115) — (Dica) $s+t$ tem um fator que não está dentre os fatores de A.

Resp. (Ex. 116) — mas não ambos. Logo, nenhum primo divide $s+t$, e $s+t>1$ seria um novo primo, não listado antes.

Resp. (Ex. 117) — (Dica) Se $3 \mid a$, então $9 \mid a^2$.

Resp. (Ex. 124) — Ache o expoente de 2 na fatoração de $\binom{100}{n}$.

Resp. (Ex. 126) — Semelhante à demonstração da infinitude dos primos $4k+3$.

Resp. (Ex. 130) — $6/\pi^2$.
Para resolver: comece olhando para a probabilidadede um inteiro qualquer k dividir os dois números; a de um número ser o MDC de ambos; e a desse último número ser 1.

Resp. (Ex. 136) — É uma tripla pitagórica primitiva. Considere x, y, z módulo 3. Como $2 \equiv -1 \pmod 3$, cada variável é ± 1 ou zero módulo 3.
Primeiro, não existe o caso em que todos são divisíveis por 3, porque $\operatorname{mdc}(x,y,z) = 1$.
Assim, não é possível que tanto $3 \mid x$ como $3 \mid y$, porque se assim fosse, $3 \mid z$ e cairíamos no mesmo problema ($\operatorname{mdc}(x,y,z) = 1$).
Agora, por absurdo, suponha que nem x nem y sejam zero módulo 3 (ou seja, $3 \nmid x$, $3 \nmid y$). Então

$$x, y \equiv \pm 1 \pmod 3$$

Isso porque

$$x^2 + y^2 = 3k+2, z^2 \qquad\qquad = 3r+1 \text{ ou } 3r.$$

porque $(\pm 1)^2 = +1$.
Mas então,

$$\begin{aligned} x^2 + y^2 &= z^2 \\ 3k+2 &= 3r+1 \text{ ou } 3r \\ 3(k-r) &= 1-2 \text{ ou } -2 \\ 3(k-r) &= -1 \text{ ou } -2, \end{aligned}$$

e $3 \mid -1$ ou $3 \mid -2$, o que é impossível.
Em toda tripla pitagórica, portanto, 3 divide um dentre x e y.

Resp. (Ex. 137) — (Dica) Escreva

$$\left(\frac{m}{n}\right)^2 + \left(\frac{r}{s}\right)^2 = 3,$$

presumindo $m, n, r, s \in \mathbb{Z}$ e $\mathrm{mdc}\,(m, n) = \mathrm{mdc}\,(r, s) = 1$. Logo,

$$m^2 + r^2 = 3z^2,$$

com $\mathrm{mdc}\,(m, r, z) = 1$.
Se os racionais propostos existem, então a equação também deve valer módulo 3.

$$\begin{aligned} m^2 + r^2 &\equiv 3 \pmod 3 \\ m^2 + r^2 &\equiv 0 \pmod 3 \end{aligned}$$

Resp. (Ex. 138) — Reveja a demonstração do Teorema de Wilson.

Resp. (Ex. 147) — A equação diofantina tem soluções, mas nenhuma com x e y positivos:

$$-22(30) + 44(18) = 132$$

A forma geral da solução é

$$30(-22 + 18k) + 18(44 - 30k) = 132$$

Mas precisamos então de

$$\begin{aligned} -22 + 18k &> 0 \\ 44 - 30k &> 0 \end{aligned}$$

Ou seja,

$$\begin{aligned} k &> \frac{22}{18} \approx 1.222 \\ k &< \frac{44}{30} \approx 1.466, \end{aligned}$$

e não existe $k \in \mathbb{Z}$ que possamos usar.

Resp. (Ex. 148) — $k > -30.75$, e como k deve ser inteiro, $k \geq -30$.

Resp. (Ex. 151) — Está claro, pela presença de "$(p-1)!$" no enunciado, que o teorema de Wilson será usado. O expoente $p-1$ indica que o pequeno teorema de Fermat (ou o de Euler) também é útil.

Resp. (Ex. 152) — Escreva $(p-1)!$, escreva $(p-1)!/(p-n)!$, use o teorema de Wilson.

Resp. (Ex. 168) — Lembre que dois uns consecutivos reiniciam a sequência.

Resp. (Ex. 175) — $\{-13, -11, -9, -7, -5, -3, -1, 1, 3, 5, 7, 9, 11\}$.

Resp. (Ex. 179) — $p \mid k^2 - 1 = (c-1)(c+1)$, logo pelo Lema de Euclides, $p \mid c+1$ ou $p \mid k-1$

Resp. (Ex. 184) — Não é um grupo. Na tabela,

$$ab = c$$
$$ac = d$$

Então

$$a\underline{ab} = ac = d,$$

mas

$$\underline{aa}b = eb = b,$$

e como a operação não é associativa – $a(bb) \neq (aa)b$ – teríamos $b = d$.

Resp. (Ex. 185) — Não – mostre que não são incongruentes $\pmod m$.

Resp. (Ex. 187) — ϕ é multiplicativa; $g^{2p^k} - 1$ é par ou ímpar? O que significa $g^{2p^k} \pmod{2p^k}$?

Resp. (Ex. 189) — Qual é a ordem de $a^m - 1$ módulo m?

Resp. (Ex. 201) — $(x, y) \odot (a, b) = (ax - by, ay + bx)$

Resp. (Ex. 202) — Reveja o exemplo de raízes da unidade, com $m = 12$. Ou ainda, considere o sistema reduzido de resíduos módulo 15:

$$S = \{1, 2, 4, 7, 8, 11, 13, 14\}.$$

Veja agora as duas maneiras de dispor os elementos:

$$\begin{array}{cc} 1 & 2 \\ 4 & 8 \\ 7 & 11 \\ 13 & 14 \end{array}$$

As linhas são sistemas reduzidos de resíduos. Veja também

$$\begin{array}{cccc} 1 & 2 & 4 & 8 \\ 11 & 7 & 14 & 13 \end{array}$$

Este exercício é desenvolvido como parte do texto no livro de Tom Apostol[31]

Resp. (Ex. 205) — (Dica) Ordem do grupo de unidades. Teorema de Lagrange.

Resp. (Ex. 207) — $\sigma(p^n) = \frac{p^{n+1}-1}{p-1}$ $d(p^n) = n + 1$

Resp. (Ex. 208) — Trivial, usando o Exercício 207.

Resp. (Ex. 209) — $n = ab$. $\sigma(n) > n + a + b + 1$. Se $a < \sqrt{n}$, então o que ocorre com b?

Resp. (Ex. 210) — 10 e 49 apenas.

Resp. (Ex. 211) — Os primos que dividem n podem ser $2, p_1, p_2, \ldots$ Então os divisores são $1, 2^2, 2^3, \ldots, p_1, p_1^2, \ldots, p_2, p_2^2, \ldots$. Escreva $\sigma(n)$:

$$\sigma(n) = (1 + 2 + 2^2 + \cdots)(p_1 + p_1^2 + \cdots)(p_2 + p_2^2 \cdots) \cdots$$

[31] **Apostol**, Tom. **Introduction to Analytic Number Theory**. New York, NY: Springer, 1976.

Determine a paridade dos fatores.

Resp. (Ex. 217) — ϕ é multiplicativa; $\mathrm{mdc}\,(2, k) = 1$ se k é ímpar...

Resp. (Ex. 225) — É um par de Moebius.

Resp. (Ex. 229) — $n \leq 2^{\pi(n)}\sqrt{n}$, e depois chegue a $2^{\pi n} \geq \sqrt{n}$, e $\pi(n) \geq \log \sqrt{n}$.

Resp. (Ex. 234) — (a) $a = 3, b = 2$. (b) 17 é primo...

Resp. (Ex. 239) — Investigue o conjugado de raizes primitivas da unidade.

Resp. (Ex. 243) — 15 (use de Polignac-Legendre).

Resp. (Ex. 244) — 9 (use de Polignac-Legendre).

Resp. (Ex. 256) — (i) use a fórmula para a soma dos n primeiros quadrados; (ii) lembre que os resíduos quadráticos são distribuídos simetricamente ao redor de zero (ou, equivalentemente, ao redor de $(p-1)/2$).

Resp. (Ex. 260) — Pense na existencia de raiz quarta primitiva da unidade em U_p.

Resp. (Ex. 264) — Observe os divisores de $5(n!)^2 - 1$. Há um divisor $p > n$ que não é $5k + 1$.

Resp. (Ex. 275) — Não é (ou seja, $(17/401) = -1$). Use a lei da reciprocidade quadrática e propriedades do símbolo de Jacobi.

Resp. (Ex. 282) — É consequência do Teorema 10.9.

Resp. (Ex. 285) — (i) Use (após demonstrar) a identidade de Brahmagupta-

Fibonacci, ou (ii) Considere o complexo $z = (a + bi)(c + di)$. Qual é a norma de z?

Resp. (Ex. 286) — ($\Rightarrow$) $m = a^2 - b^2 = (a+b)(a-b)$. Mas a diferença entre estes dois fatores é $(a+b)-(a-b) = -2b$, e os dois tem a mesma paridade.
($\Leftarrow$) Suponha $m = pq$, onde p, q tem a mesma paridade.
Caso um: p, q ímpares.
$p + q$ e $p - q$ são pares, e existem inteiros

$$a = \frac{p+q}{2}, \quad b = \frac{p-q}{2}.$$

Verifique que $a^2 - b^2 = pq = m$. Caso dois: p, q pares.
Sejam $p = 2u$ e $q = 2w$. Então $m = pq = 4(uw)$. Então

$$(u + w)^2 - (u - w)^2 = 4uv = m.$$

Resp. (Ex. 287) — Parta de

$$n = \frac{a^2}{b^2} + \frac{c^2}{d^2}$$

e chege a

$$nb^2 = \text{alguma soma de dois quadrados } \textbf{de inteiros}$$

depois argumente que nb^2 é representável; que por isso nb^2 (e consequentemente n) não tem fatores $4k + 1$.

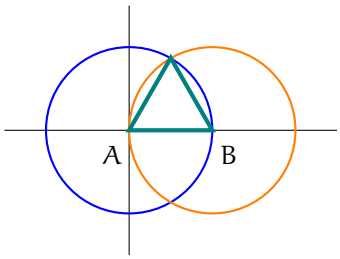
Resp. (Ex. 292) — Comece com $4^a(8k + 7) = 4^a(8k + 6) + (2^a)^2$. Depois, $4^a(8k + 6) + (2^a)^2 = x^2 + y^2 + z^2$. Com $w = 2^a$ o resultado segue.

Resp. (Ex. 295) — Não e não.

Resp. (Ex. 316) — O sucessor do primo é par.

Resp. (Ex. 340) — Expresse as extremidades do intervalo como frações contínuas. Encontre o primeiro termo em que diferem e adicione 1 ao menor deles, a não ser que seja o último. Descarte os termos à direita. O que resta?

Resp. (Ex. 346) —



Resp. (Ex. 348) — Claramente, $\sqrt[3]{2} \notin \mathcal{C}$, mas $\sqrt[3]{2} \in \mathcal{A}$. Além disso, da demonstração do Teorema 16.4, todo número construtível é algébrico. Portanto,

$$\mathcal{C} \subset \mathcal{A}$$

Produção do Livro

Este texto foi produzido inteiramente em LaTeX em um sistema Debian GNU/Linux. Os diagramas foram criados sem editor gráfico, usando diretamente o pacote Ti*k*Z. O ambiente Emacs foi usado para edição do texto LaTeX.

Índice Geral

$GL(n, F)$, 332
$M(n)$, 238
$N(n)$, 286
$P(n)$, 286
$PSL(2, \mathbb{Z})$, 332
$R(n)$, 286
$R_{n\times n}$, 239
$SL(n, F)$, 332
$[x]$, 224
Δ, 303
Γ, 332
$\lceil x \rceil$, 224
δ
    de Kronecker, 200
$\lfloor x \rfloor$, 224
$\mathbb{Z}/n\mathbb{Z}$, 121
$\mathbb{Z}[\omega]$, 347
$\mathbb{Z}_n$, 121
$\mu(n)$, 214
ω, 347
ϕ (irracionalidade), 383
$\phi(n)$, 201
π (irracionalidade), 381
$\pi(n)$, 229
    crescimento de, 231
$\mathcal{O}_F$, 348
Q_n, 241
$\mathrm{rad}(n)$, 235
$\mathbb{Q}[\sqrt{d}]$, 343
$\sigma(n)$, 201
$\sim$, 301
$\mathbb{H}$, 333
U_n, 187
$a^{(i)}$, 364
$d(n)$, 201
e (irracionalidade), 376
$p(n)$, 353
p_i/q_i, 364
$r(n)$, 286
$w(f)$, 312

algoritmo
    de Euclides (complexidade), 78
    de Euclides (para o MDC), 65
anel, 34, 35
    de inteiros quadráticos, 348
    dos inteiros módulo n, 121
aritmética
    nos inteiros, 33
    nos naturais, 17
automorfismo
    de forma quadrática, 312
axioma, 5
axiomas
    de Dedekind-Peano, 6
    independência, 8

base, 41
    de reticulado, 79
base 13
    função, 47
boa ordem (princípio da), 22
Brahmagupta-Fibonacci
    identidade de, 276
Bézout

coeficientes de, 68
Lema de, 61

Chebychev
teorema de, 231
co-primos, 93
coeficientes parciais (de fração contínua), 359
combinação linear inteira, 61
complexidade
do algoritmo de Euclides, 78
composição
de formas quadráticas, 318
composto
em anel de inteiros quadráticos, 349
congruência, 120
linear em n variáveis, 150
não linear, polinomial, 151
polinomial, 151
conjugado
em corpo quadrático, 344
construção
com régua e compasso, 389
conteúdo de polinômio, 113
convergente, 364
convolução de Dirichlet, 212
Conway
função base 13, 47
corpo, 34, 37
dos números tropicais, 38
extensão de, 341
quadrático, 343
quadrático imaginário, 343
quadrático real, 343
crescimento de $\pi(n)$, 231
critério de Euler, 241

de Moivre
fórmula de, 188
delta
de Kronecker, 200
descida infinita, 24
determinante
de forma quadrática, 298
diagrama de Ferrer, 353
Dirichlet
convolução de, 212
discriminante, 298, 303
fundamental, 307
divide, 57
para inteiros quadráticos, 348
divisão, 60
domínio Euclideano, 85
domínio fundamental, 334

Eisenstein
demonstração da Lei da Reciprocidade Quadrática, 254
Lema de, 255
elemento irredutível, 111
equação diofantina, 133
linear, 133
equivalência
de pontos em $\mathbb{H}$, 333
espaço métrico, 374
completo, 374
Euclides
algoritmo de (complexidade), 78
algoritmo de (para o MDC), 65
algoritmo estendido de, 68
lema de, 64
Euler
critério de, 241
Teorema de, 171
extensão
de corpo, finita, 342
de corpo, grau de, 342
extensão de corpo, 341
extensão de um corpo, 341

fatoração única, 94
Fermat

método da descida infinita, 24
número de, 101
pequeno Teorema de, 172
primo de, 101
Ferrers
diagrama de, 353
Fibonacci
coelhos imortais, 73
números de, 73
números, módulo m, 160
período d esequencia módulo m, 161
sequência de, 73
forma bilinear, 295
simétrica, 296
forma quadrática, 296
binária, 295, 296, 302
determinante, 298
grau de, 296
principal, 303
reduzida (positiva definida), 309
semirreduzida (positiva definida), 309
ternária, 321
ternária integral, 321
formas modulares, 331
formas quadráticas
composição de, 318
concordantes, 318
definidas, 299
indefinidas, 299
formas quadráticas binárias
equivalentes, 301
fração contínua
coeficientes parciais, 359
eventualmente periódica, 371
finita, 359
infinita, 363
infinita simples, valor de, 367
simples, 359
função
aritmética, 200
base 13 de Conway, 47
de Mangoldt, 222
de Merten, 238
geradora, 352
multiplicativa, 207
funções aritméticas, 199
fórmula
de de Moivre, 188

Gauss
demonstração da Lei da Reciprocidade Quadrática com raízes da unidade, 260
demonstração da Lei da Reciprocidade Quadrática por indução, 250
Lema de, 271
Lema de, para polinômios, 114
soma de, 261
geometria hiperbólica, 8
gerador de grupo, 185
grau
de extensão de corpo, 342
de forma quadrática, 296
grau de congruência polinomial, 151
grupo, 181
abeliano, 181
comutativo, 181
cíclico, 185
de resíduos quadráticos módulo n, 241
de unidades de inteiros quadráticos, 349
de unidades módulo n, 187
linear especial, 332
linear geral, 332
modular, 332
grupo modular, 331

Hensel
    Lema de, 152

identidade
    de Brahmagupta-Fibonacci, 276
inclusão-exclusão - em nota de rodapé, 204
indução finita, 9
integral
    forma quadrática ternária, 321
inteiro
    em corpo quadrático, 345
    Gaussiano, 79
    Gaussiano (norma de), 81
    quadrático, 345
inteiros, 30
    racionais, 30
invariante, 303
inverso módulo m, 124
irracional
    quadrático, 371
irracionalidade
    de ϕ, 383
    de π, 381
    de $\sqrt{2}$, 362
    de e, 376

Kronecker
    δ de, 200

Legendre-de Polignac
    Teorema (fórmula de), 226
Lema
    de Bézout, 61
    de Eisenstein, 255
    de Euclides, 64
    de Gauss, 271
    de Gauss para polinômios, 114
    de Hensel, 152
Lucas
    Teorema de, 116

Mangoldt
    função de, 222
matriz
    de Redheffer, 239
meio-plano superior, 333
melhor aproximação, 368
menor ou igual, 20
Mersenne
    número de, 98
    primo de, 98
Merten
    função de, 238
Moebius
    Teorema (fórmula) da inversão, 217
multiplicação (de naturais), 18
máximo divisor comum, 60
métrica, 374
mínimo múltiplo comum, 70

norma
    de inteiro Gaussiano, 81
    em corpo quadrático, 344
    em domínio Euclideano, 85
número
    de classe de discriminante fundamental, 314
    de Fermat, 101
    de Fibonacci, 73
    de Mersenne, 98
    inteiro, 33
    inteiro Gaussiano, 79
    irracional quadrático, 371
    perfeito, 98
    triangular, 14
números
    construtíveis, 390
    de Fibonacci, módulo m, 160
    inteiros, 30
    irracionais, 362
    naturais, 6
    racionais, 30
    tropicais (corpo dos), 38

ordem
    de elemento em sistema de resíduos, 173
    de raiz da unidade, 192
    parcial, 21
ordem de p em n, 96
ordenação dos naturais, 20

par de Moebius, 218
partição, 30
partição de um inteiro, 352
partições de um inteiro, 351
    representação gráfica, 353
Pascal
    triângulo de, 10, 116
pertinência a expoente módulo m, 173
período
    de Pisano, 161
    de sequência de Fibonacci módulo m, 161
Pisano
    período de, 161
plano complexo, 79
polinômio
    conteúdo de, 113
    primitivo, 113
polinômios
    congruentes módulo p, 156
    equivalentes módulo p, 156
    reduzidos módulo p, 156
primo, 93
    das formas $4n + 1$ e $4n + 3$, 107
    de Fermat, 101
    de Mersenne, 98
    em anel de inteiros quadráticos, 349
primorial, 102

quociente, 60

racionais, 30
radical, 235
raiz da unidade, 188
    ordem de, 192
raiz primitiva, 172
raiz primitiva da unidade, 192
razão áurea, 74
raízes da unidade
    demonstração da Lei da Reciprocidade Quadrática, 260
reciprocidade quadrática, 245
    demonstração de Gauss com raízes da unidade, 260
    demonstração de Gauss por indução, 250
    demonstração de Rousseau, 251
    demonstração geométrica de Eisenstein, 254
    Teorema da, 246
Redheffer
    matriz de, 239
região fundamental, 334
relação
    de equivalência, 31
    de ordem parcial, 21
representação
    de inteiro como dois quadrados, 273
    de inteiro por forma quadrática, 300
    própria de inteiro como dois quadrados, 273
    regular, 344
resto, 60
resíduo quadrático, 241
reticulado, 79
Rousseau
    demonstração da Lei da Reciprocidade Quadrática, 251
régua e compasso
    construção com, 389

sequência de Cauchy, 374

sistema completo de resíduos, 168
sistema reduzido de resíduos, 168
solução singular para congruência polinomial, 152
soma (de naturais), 18
soma de dois quadrados, 273
soma de Gauss, 261
soma de quadrados, 273
soma de quatro quadrados, 279
soma de três quadrados, 283
subgrupo, 186
sucessor, 7
série formal de potências, 352
símbolo
  de Jacobi, 243
  de Legendre, 243

Teorema
  Chinês dos restos, 137
  da inversão de Moebius, 217
  da reciprocidade quadrática, 246
  de Chebychev, 231
  de Euler, 171
  de Fermat (pequeno), 172
  de Legendre-de Polignac, 226
  de Lucas, 116
  de Wilson, 128
  do valor intermediário, 47
  fundamental da aritmética, 96
transformação linear fracionária, 331
traço, 344
tripla pitagórica, 25
triângulo
  retângulo, 25
triângulo de Pascal, 10, 116
tropicais
  corpo dos números, 38

um (definição como sucessor do zero), 18
unidade
  em anel, 35
  em grupo de inteiros quadráticos, 348

valor de fração contínua infinita simples, 367
valor intermediário
  teorema, 47

Wilson
  Teorema de, 128

Índice de Pessoas

Abel, N. H., 181
Al-Fārisī , 94
Al-Haytam, 137
Al-Khwarizmi, 137
Āryabhaṭa , 137
Bachet. C. G., 61, 119, 133, 279
Benford, F., 52
Bertrand, Joseph, 230
Bézout, Étienne, 61
Bhaskara, 137
Bolyai, János, 8, 9
Brahmagupta, 129, 140
Cauchy, A. L., 181
Chebychev, P. L., 230
Chevalley, C., 158
Conway, John, 47
Dedekind, Richard, 6, 146
de Moivre, Abraham, 188
Diofanto, 3, 94, 132
Dirichlet, P. G. L., 200, 317
Eisenstein, F. G. M., 254
Erdös, Paul, 104
Euclides, 63, 65, 93, 94, 103
Euler, L., 167, 171, 175, 188, 199
Fibonacci, Leonardo, 73
Fourier, J. B. J., 379
Fraenkel, Abraham, 7
Galois, E., 181
Gauss, J. C. F., 9, 94, 167, 175, 189, 205, 214, 316
Gödel, Kurt, 6
Hardy, G. H., 52
Cohn, H., 377
Hensel, Kurt, 152
Hermite, Charles, 104
Kronecker, L., 146
Lagrange, Joseph Louis, 127, 187, 279
Lambert, J. H., 175, 382
Lobachevsky, Nikolai, 8, 9
Lucas, É., 116
von Mangoldt, H. C. F., 222
Mersenne, M., 98
Möbius, A. F., 214
Newcomb, Simon, 52
Newton, Isaac, 154, 188
Noether, A. E., 146
Pascal, Blaise, 10
Peano, Giuseppe, 6
Pierce, Charles Sanders, 6
Qín Jisháo, 137, 139
Raphson, J., 153
Riemann, Bernhard, 200
Robbins, Neville, 108
Russel Bertrand, 6
Simon, Imre, 38
Skolem, Thoralf, 7
Sūnzǐ , 138, 167
Taurinus, Franz, 9
Yī Xíng , 137
Ibn Yunus, 137
Zermelo, Ernst, 7

Referências

Agargün, Ahmet G.; **Fletcher, Colin**. al-Fārisī and the Fundamental Theorem of Arithmetic. **Historia Mathematica**, v. 21, p. 162–173, 1994. Página 94.

Andrews, George. **Number Theory**. New York: Dover, 1994. Página 42.

Apostol, Tom. **Introduction to Analytic Number Theory**. New York, NY: Springer, 1976. Página 411.

Bachet, Claude Gaspar (Sr de Meziriac). **Problèmes plaisans et deléctables, qui se font par les nombres**. [*S. l.*], 1612. Disponível em `https://archive.org/details/bub_gb_Zy0PAAAAQAAJ`. Página 61.

Bag, Amulya Kumar. Binomial theorem in ancient India. **Indian Journal of History of Science**, v. 1, n. 1, p. 68–74, 1966. Página 11.

Baumgart, Oswald. **The Quadratic Reciprocity Law: a collection of classical proofs**. [*S. l.*]: Birkhauser, 2015. Página 245.

Benford, Frank. The Law of Anomalous Numbers. **Proceedings of the American Philosophical Society**, v. 78, n. 4, p. 551–572, 1938. Página 52.

Bennet Jr, Albert B. Visualizing the Geometric Series. **The Mathematics Teacher**, v. 82, n. 2, p. 130–136, 1989. Página 13.

Bernays, Paul; **Fraenkel, Abraham**. **Axiomatic Set Theory**. [*S. l.*]: North-Holland, 1958. Página 7.

Bézout, Etienne. **Théorie Générale des Équations Algébriques**. [*S. l.*], 1779. Disponível em `https://archive.org/details/thoriegnra00bz`. Página 61.

Bondarenko, Boris. **Generalized Pascal Triangles and Pyramids**. [*S. l.*]: The Fibonacci Association, 1993. Disponível em https://www.fq.math.ca/pascal.html. Página 11.

Boyer, Carl B. A History of Mathematics. [*S. l.*]: Wiley, 1991. Página 41.

Brahmagupta. **Brahmasphuta Siddhanta (Brāhmasphuṭasiddhānta)**. [*S. l.: s. n.*]. Página 140.

Brezinski, Claude. **History of Continued Fractions and Padé Approximants**. Berlin Heidelberg: Springer-Verlag, 1991. Página 359.

Brink, David. New light on Hensel's lemma. **Expositiones Mathematicae**, v. 24, n. 4, p. 291–306, 2006. Página 152.

Buell, Duncan A. Binary Quadratic Forms. New York, NY: Springer-Verlag, 1989. Página 295.

Bullynck, Maarten. Modular arithmetic before C.F. Gauss: Systematizations and discussions on remainder problems in 18th-century Germany. **Historia Mathematica**, v. 36, p. 48–72, 2009. Página 119.

Burton, David. The History of Mathematics: An Introduction. *In:* 6. ed. [*S. l.*]: McGraw-Hill, 2006. 11 - Nineteenth-Century Contributions: Lobachevsky to Hilbert. Página 9.

Bussey, W. H. Fermat's Method of Infinite Descent. **The American Mathematical Monthly**, v. 25, n. 8, p. 333–337, 1918. Página 24.

Bussey, W. H. The Origin of Mathematical Induction. **The American Mathematical Monthly**, v. 24, n. 5, p. 199–207, 1917. Página 10.

Cassels, J. W. S. Rational Quadratic Forms. London: Academic Press, 1978. Página 317.

Cataldi, Pietro Antonio. **Trattato del modo brevissimo di trouare la radice quadra delli numeri, et regole da approssimarsi di coninuo al vero nelle radice delli numeri non quadrati, con le cause, et inventioni loro. Et anco il modo di pigliarne la radice cuba, applicando il tutto alle operationi militari et altre**. [*S. l.: s. n.*], 1613. Sim, o título tem 48 palavras. Disponível em https://archive.org/details/hin-wel-all-00000163-001/page/n8/mode/2up. Página 360.

Chevalley, C. Démonstration d'une hypothèse de M. Artin. **Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg**, v. 11, p. 73–75, 1935. Página 159.

Colebrooke, Henry Thomas. **Algebra, with Arithmetic and mensuration, from the Sanscrit of Brahmegupta and Bháscara**. [*S. l.*]: London J. Murray, 1817. Disponível em https://archive.org/details/algebrawitharith00brahuoft. Página 140.

D' Alessandro, William. Proving quadratic reciprocity: explanation, disagreement, transparency and depth. **Synthese**, v. 198, p. 8621–8664, 2021. Página 249.

Dauben, Joseph W. Mathematics of Egypt, Mesopotamia, China, India, and Islam: A Sourcebook. *In:* edição: Victor Katz. [*S. l.*]: Princeton University Press, 2007. Chinese Mathematics. Página 139.

de Moivre, Abraham. **Miscellanea Analytica de Seriebus et Quadraturis**. Londres: J. Tonson & J. Watts, 1730. Página 188.

Dedekind, Richard. **Was sind und was sollen die Zahlen?** [*S. l.*], 1888. Publicado como brochura. Página 6.

Dickson, Leonard Eugene. **History of The Theory of Numbers**. New York, N.Y.: Chelsea Publishing Company, 1971. v. 2. Página 137.

Diophantus. **Diophanti Alexandrini opera omnia cum Graecis commentariis**. Edição: P. Tannery. [*S. l.*]: Stutgardiae Teubner, 1895. v. 1. Disponível em https://archive.org/details/diophantialexan03plangoog/. Página 133.

Diophantus. **Diophanti Alexandrini opera omnia cum Graecis commentariis**. Edição: P. Tannery. [*S. l.*]: Stutgardiae Teubner, 1895. v. 2. Disponível em https://archive.org/details/diophantialexan00plangoog. Página 133.

Dirichlet, Johann Peter Gustav Lejeune. **De formarum binariarum secundi gradus compositione**. [*S. l.: s. n.*], 1851. Reproduzido em Jour. fur Math., 47, 1854, 155-160; Werke, II, 1897, 105-114. Trad Francês, Jour, de Math., (2), 4, 1859, 389-398. Página 317.

Dirichlet, L. Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sing, unendlich viele Primzahlen erhält.

Abhandlungen der Königlich Preußischen Akademie der Wissenschaften, p. 45–81, 1837. Página 200.

Euclid. **The Elements**. [*S. l.*]: Green Lion Press, 2002. Edição bilíngue Inglês/Grego. Páginas 25, 64, 65, 93, 98.

Euler, Leonhard. **Introduction in Analysin Infinitorum**. [*S. l.*], 1748. O original em Latim está disponível em `https://archive.org/details/bub_gb_jQ1bAAAAQAAJ/page/n21/`. Página 351.

Euler, Leonhard. Theoremata arithmetica nova methodo demonstrata. **Novi Commentarii academiae scientiarum Petropolitanae**, v. 8, p. 74–104, 1763. Página 171.

Euler, Leonhard. Variae observationes circa series infinitas. **Commentarii academiae scientiarum Petropolitanae**, v. 9, p. 160–188, 1744. Página 199.

Flath, Daniel. **Introduction to Number Theory**. [*S. l.*]: John Wiley e Sons, 1989. Página 250.

Gauss, Johann Carl Friedrich. **Disquisitiones Arithmeticae**. [*S. l.*], 1801. Páginas 119, 189, 205, 237, 245, 285, 303, 317.

Gauss, Johannes Carl Friedrich. Theoria residuorum biquadraticorum. Commentatio secunda. **Comm. Soc. Reg. Sci. Göttingen**, v. 7, p. 89–148, 1831. Página 80.

Goldman, Jay R. The Queen of Mathematics: A Historically Motivated Guide to Number Theory. Natick, MA: A. K. Peters, 1998. Páginas 95, 245, 260.

Gouvêa, Fernando. Review of
The quadratic reciprocity law: A collection of classical proofs, by Oswald Baumgart (F. Lemmermeyer, Ed. and Trans.) **MAA Reviews**, 2015. Página 249.

Gueron, Eduardo; **Pellegrini, Jerônimo**. Application of Benford − Newcomb law with base change to electoral fraud detection. v. 607, 2022. Preprint disponível em `https://arxiv.org/abs/2207.05524v2`. Página 53.

Gueron, Eduardo; **Pellegrini, Jerônimo**; **Aristimunha, Bruno**. Distribuição de Newcomb-Benford, Mudanças de Bases e Aplicações Eleitorais. *In:* 1. PROCEEDING Series of the Brazilian Society of

Computational and Applied Mathematics. Bonito - MS: [*s. n.*], 2023. v. 10. Trabalho apresentado no XLII CNMAC. Página 53.

Hardy, G. H. A Mathematician's Apology. [*S. l.*]: Cambridge University Press, 1940. Página 52.

Hardy, G. H.; **Wright, E. M. An Introduction to The Theory of Numbers**. 6. ed. [*S. l.*]: Oxford, 2009. Página 214.

Hardy, Michael; **Woodgold, Catherine**. Prime Simplicity. **The Mathematical Intelligencer**, v. 31, n. 4, p. 44–52, 2009. Página 103.

Heath, Thomas L. Diophantus Of Alexandria A Study In The History Of Greek Algebra. [*S. l.: s. n.*], 1910. Disponível em https://archive.org/details/in.ernet.dli.2015.154147. Página 133.

Hensel, Kurt. Neue Grundlagen der Arithmetik. **Journal für die reine und angewandte Mathematik**, v. 127, p. 51–84, 1904. Página 152.

Hiscocks, John. Triangle Numbers in the History of Mathematics. **Teaching Mathematics and its Applications**, v. 9, n. 2, 1990. Página 14.

Kennedy, Evelyn. Omar Khayyam. **The Mathematics Teacher**, v. 59, n. 2, p. 140–142, 1966. Página 11.

Kleiner, Israel. **Excursions in the History of Mathematics**. [*S. l.*]: Birkhauser, 2012. Página v.

Lagrange, Joseph-Louis. Démonstration d'un théorème d'arithmétique. **Nouveaux mémoires de l'Académie royale des sciences et belles-lettres de Berlin**, p. 122–133, 1770. Página 279.

Lagrange, Joseph-Louis. **Ouvres de Lagarange**. Edição: M. J.-A Serret. [*S. l.*]: Gauthier Villars, 1867. v. 3. Página 279.

Landau, Edmund. **Elementary Number Theory**. New York, NY: Chelsea Publishing Company, 1958. Página 323.

Legendre, Adrien-Marie. **Essai sur la théorie des nombres**. [*S. l.*]: Paris, Duprat, 1798. Disponível em https://archive.org/details/essaisurlathor00lege. Página 284.

Lemmermeyer, Franz. **Reciprocity Laws: from Euler to Eisenstein**. [*S. l.*]: Springer, 2000. Página 245.

Libbrecht, Ulrich. **Chinese Mathematics in the Thirteenth Century: the Shu-shu chiu-chang of Ch'in Chiu-shao**. [*S. l.*]: MIT, 1973. Página 139.

Martzloff, Jean-Claude. **A History of Chinese Mathematics**. [*S. l.*]: Springer, 2006. Página 11.

Maurolycus, Franciscus. **Arithmeticorum libri duo**. [*S. l.*], 1575. Incluso na obra "D. Francisci Maurolyci Opuscula mathematica". Página 10.

Mendelson, Eliott. **Introduction to Mathematical Logic**. 6. ed. [*S. l.*]: CRC Press, 2015. Página 6.

Mersenne, Marini. **Cogitata Physica-Mathematica**. [*S. l.*], 1644. `https://archive.org/details/fmarinimersennic00mers`. Página 98.

Newcomb, Simon. Note on the Frequency of Use of the Different Digits in Natural Numbers. **American Journal of Mathematics**, v. 4, n. 1, p. 39–40, 1881. Página 52.

Newton, Isaac. **The Method of Fluxions and Infinite Series: With Its Application to the Geometry of Curve-lines**. [*S. l.: s. n.*], 1736. "By Sir Isaac Newton, Translated from the Author's Latin Original Not Yet Made Publick. To which is Subjoin'd, a Perpetual Comment Upon the Whole Work, By John Colson, Sir Isaac Newton. Henry Woodfall; and sold by John Nourse". Tradução do original para o Inglês em `https://archive.org/details/methodoffluxions00newt`. O manuscrito original em Latim, com a caligrafia de Newton, "De Methodis Serierum et Fluxionum", pode ser lido em `https://cudl.lib.cam.ac.uk/view/MS-ADD-03960/100`. Página 154.

Öhman, Lars-Daniel. Are Induction and Well-Ordering Equivalent? **The Mathematical Intelligencer**, v. 41, n. 3, p. 33–40, 2019. Página 22.

Oman, Greg. The Converse of the Intermediate Value Theorem: From Conway to Cantor to Cosets and Beyond. **Missouri Journal of Mathematical Sciences**, v. 26, n. 2, p. 134–150, 2014. Página 47.

Ore, Oystein. **Number Theory and Its History**. New York: Dover Publications, 1976. Páginas 42, 127.

Pascal, Blaise. **Traite du Triangle Arithmetique, avec quelques autres petits traitez sur la mesme matiere**. Paris: Guillaume Desprez, 1665. Página 10.

Peano, Giuseppe. **Arithmetices principia, nova methodo exposita**. [*S. l.*], 1889. Disponível em Latim, com tradução para Inglês em https://github.com/mdnahas/Peano_Book. Página 6.

Peano, Giuseppe. Logique Mathématique. **Formulaire de Mathématiques**, 1897. Página 126.

Pierce, Charles Sanders. On the Logic of Number. **American Journal of Mathematics**, v. 4, n. 1, p. 85–95, 1881. Página 6.

Raphson, Joseph. **Analysis Aequationum Universalis**. [*S. l.: s. n.*], 1702. Original em Latim disponível em https://archive.org/details/bim_eighteenth-century_analysis-quationum-univ_raphson-joseph_1702. Página 153.

Rashed, Roshdi. Ibn Al-Haytham et le théorème de Wilson. **Archive for History of Exact Sciences**, v. 22, n. 4, p. 305–321, 1980. Página 126.

Riemann, Bernhard. Über die Anzahl der Primzahlen unter einer gegebenen Grösse (On the Number of Primes Less Than a Given Magnitude). **Monatsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin**, p. 671–680, 1859. Página 200.

Roque, Tatiana. **História da Matemática: uma visão crítica, desfazendo mitos e lendas**. [*S. l.*]: Zahar, 2012. Páginas 25, 41.

Rose, H. E. A Course in Number Theory. Oxford, UK: Oxford University Press, 1988. Páginas 158, 317.

Rousseau, G. On the Quadratic Reciprocity Law. **Journal of the Australian Mathematical Society**, v. 51, p. 423–425, 1991. Página 251.

Russel, Bertrand. **Introdução à Filosofia Matemática**. [*S. l.*]: Zahar, 1974. Página 6.

Sigler, Laurence. **Liber Abaci: A Translation into Modern English of Leonardo Pisano's Book of Calculation**. [*S. l.*]: Springer, 2002. Página 73.

Singh, Paramand. The So-called Fibonacci Numbers in Ancient and Medieval India. **Historia Mathematica**, v. 12, n. 3, p. 229–244, 1985. Página 73.

Skolem, Thoralf. Some Remarks on Axiomatized Set Theory. *In:* **Heijenoort, Jean van** (ed.). **Harvard University Press**. [*S. l.*]: Harvard University Press. p. 290–301. Página 7.

Sun Tzu. **A Arte da Guerra**. [*S. l.*]: Edipro, 2021. Sun é nome; Tzu é título (mestre). Edição bilíngue. Há também uma tradução para o Inglês, livremente disponível em `https://archive.org/details/in.gov.ignca.18750/page/115/mode/2up`. Página 138.

Sylvester, James Joseph. On a remarkable discovery in the theory of canonical forms and of hyperdeterminants. **Philosophical Magazine**, v. 4, n. 2, p. 391–410, 1851. Página 298.

Vacca, Giovanni. Maurolycus, the first discoverer of the principle of mathematical induction. **American Mathematical Society**, v. 16, n. 2, p. 70–73, 1909. Página 10.

Vacca, Giovanni. Sui manoscritti inediti di Leibniz. **Bollettino di bibliografia e storia delle scienze matematiche**, v. 2, p. 113–116, 1899. Página 126.

Venkov, B. A. Elementary Number Theory. Groningen: Wolters-Noordhoff, 1970. Página 317.

Wall, D. D. Fibonacci Series Modulo m. **The American Mathematical Monthly**, v. 67, n. 6, p. 525–532, 1960. Página 160.

Waring, Edward. **Meditationes Algebraicae**. 1. ed. [*S. l.*]: J. Archdeacon, 1770. Disponível em `https://archive.org/details/bim_eighteenth-century_meditationes-algebraicae_waring-edward-lucasian_1782`. Existem traduções para o Inglês. Página 126.

Waring, Edward. **Meditationes Algebraicae**. 3. ed. [*S. l.*]: J. Archdeacon, 1782. Disponível em `https://archive.org/details/bim_eighteenth-century_meditationes-algebraic_waring-edward-lucasian_1770`. Existem traduções para o Inglês. Página 127.

Warning, E. Bemerkung zur vorstehenden Arbeit von Herrn Chevalley. **Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg**, v. 11, p. 76–83, 1935. Página 159.

Weintraub, Steven H. On Legendre's Work on the Law of Quadratic Reciprocity. **The American Mathematical Monthly**, v. 118, n. 3, p. 210–216, 2011. Página 246.

Weiss, Ittay. Survey Article: The Real Numbers - a survey of constructions. **Rocky Mountain Journal of Mathematics**, v. 45, n. 3, 2015. Também disponível em https://arxiv.org/abs/1506.03467. Página 357.

Yong, Lam Lay; **Se, An Tian**. **Fleeting Footsteps**. [*S. l.*]: World Scientific Publishing Company, 2004. Páginas 138, 139.

Yong, Ke-Xin Au. **Qin Jiushao and His Mathematical Treatise in Nine Sections in Thirteenth-Century China**. 2011. Diss. (Mestrado) – University of Alberta. Página 139.

Zermello, Ernst. Investigations in the foundations of set theory. *In:* **Heijenoort, Jean van** (ed.). **From Frege to Gödel: A Source Book in Mathematical Logic, 1879 − 1931**. [*S. l.*]: Harvard University Press. p. 199–215. Página 7.

Zolotareff, G. Nouvelle démonstration de la loi de réciprocité de Legendre. **Nouvelles Annales de Mathématiques**, v. 2, n. 11, p. 354–362, 1872. Página 272.